Niveau(x) d'enseignement: 3 Numéro EDUQ : 8270365
Centre d'intérêt: 89

Thérien, Loïc.

Structures algébriques, catégories et groupements / par Loïc Thérien ; [pour la] Section enseignement. -- [Sherbrooke] : Université de Sherbrooke, Département de mathématiques, 1977.
iv, 144 p. : graph. ; 28 cm. -- (Rapport / Université de Sherbrooke, Département de mathématiques ; 20)

En tête du titre: Notes du séminaire Mat 4893 du programme de la maîtrise en enseignement à l'élémentaire (mathématique). Bibliographie: f. iii-iv.

Cote Dewey: 510.7/T399s Cote LC: QA/11

Descripteur(s): *Mathématiques *Didactique *Primaire (Niveau)

Identificateur(s) de nom: *Wittmann, Erich

Identificateur(s) de sujet: *Groupement (Concept) *Algèbre *Structure algébrique *Catégorie *Méthode axiomatique

Notes de séminaire portant sur: 1. les structures algébriques (approche historique pour expliquer l'évolution de l'enseignement des mathématiques au primaire et justifier l'usage des ensembles, des relations et de la logique; notion de structure, types et exemples); 2. les catégories et groupements (historique du langage des catégories; langage des catégories; groupements au sens catégorique; exemples de groupements; classification et représentation réduites de groupements selon Wittmann).

Type de document: r
Financement: Bénéficiaire - Université de Sherbrooke
Organisme(s) source(s) - MEQ-DGES
Programme(s) de subvention - FCAC
Auteur de l'analyse: jr

E D U Q 8270365

UNIVERSITÉ DE SHERBROOKE

Novembre 1977 Rapport no. 20

STRUCTURES ALGEBRIQUES, CATEGORIES ET GROUPEMENTS

par

Loic Thérien

Faculté des sciences Département de mathématiques

E D U Q 8270365

SECTION ENSEIGNEMENT

Notes du Séminaire Mat 4883
du programme de la
Maîtrise en enseignement à l'élémentaire
(mathématique)

Novembre 1977 Rapport no. 20

STRUCTURES ALGEBRIQUES, CATEGORIES ET GROUPEMENTS

par

Loic Thérien

Document de travail
dans le cadre d'un projet de recherche
subventionné par le programme FCAC
du Ministère de l'Education du Québec

Plan du cours MAT 4883

Chapitre I: Structures algébriques 1

§1. Approche historique de la méthode axiomatique. 1

§2. Notion de structure. Types et exemples: 49

1. Groupes 50
2. Les anneaux 66
3. Corps 67
4. Espaces vectoriels sur un corps 68

Chapitre II: Catégories et groupements 81

§1. Historique du langage des catégories 81

§2. Langage des catégories 83

§3. Groupements (au sens catégorique) 94

§4. Exemples de groupements 102

§5. Classification et représentations réduites de groupements selon Wittmann (1975) 114

Annexe: Un exemple de groupement arithmétique 121

BIBLIOGRAPHIE

Histoire

(1) Morris Kline,
Mathematical Thought from Ancient to Modern Times,
Oxford University Press.

(2) Scientific American,
Mathematics in the Modern World,
W.H. Freeman and Co.

Catégories et groupements

(1) S. McLane,
Categories for the working mathematician,
Springer Verlag.

(2) E. Wittmann,
Natural Numbers and groupings,
Educational Studies in Mathematics, 6, 1975,
53-75.

Fondements

(1) Wilder,
Introduction to the foundations,
Wiley.

Structures algébriques

(1) Lentin et Rivaud,
Leçons d'algèbre moderne,
Vuibert

(2) A Kaufmann,
Cours de mathématiques nouvelles,
Dunod

(3) S. McLane et G. Birkhoff,
Algebra,
McMillan

(4) Moston, Sampson, Mayer,
Fondamental Structures of Algebra,
McGraw-Hill.

CHAPITRE I: STRUCTURES ALGEBRIQUES

§1. Approche historique de la méthode axiomatique.

Cette section a pour but d'utiliser l'histoire pour expliquer l'évolution de l'enseignement des mathématiques à l'élémentaire et répondre à certaines questions:

Pourquoi enseigne-t-on les ensembles, les relations et la logique?

Pourquoi ce vocabulaire moderne et ce degré d'abstraction?

Pourquoi parlons-nous aujourd'hui de concepts unificateurs?

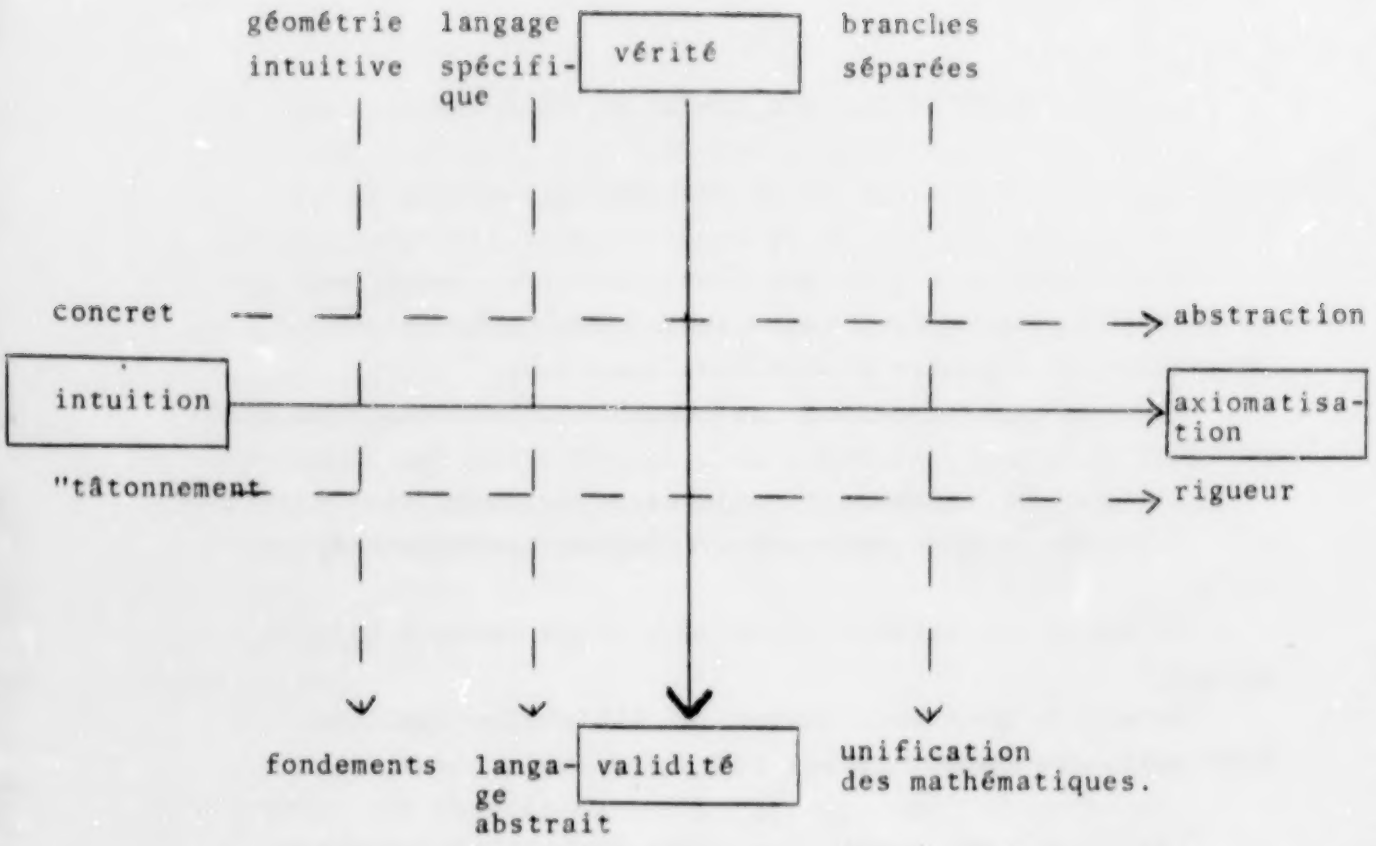
Pourquoi les mathématiques sont-elles devenue <u>la mathématique</u>?

Autant de questions auxquelles l'histoire appliquée aux fondements des mathématiques peut répondre.

Les fils conducteurs dans cette recherche historique seront constitués par la progression:

- de l'axiomatique
- du souci de rigueur
- du degré d'abstraction
- du souci d'unification des branches mathématiques.

On peut dégager deux axes principaux (le troisième axe étant le développement interne des mathématiques) dans cette recherche auxquels se greffent des axes parallèles:



L'axe horizontal pourrait représenter l'abstraction progressive interne, l'axe vertical pourrait représenter l'abstraction progressive externe.

La citation suivante de Russel résume ces deux axes:

"Les mathématiques pures constituent le sujet pour lequel nous ne savons pas de quoi l'on parle (⟶), ni si ce qu'on en dit est vrai (↓)".

Nous nous concentrerons dans cette recherche sur trois moments importants de l'histoire mathématique, que l'on peut qualifier de crises de l'intuition:

a) Les paradoxes causés par la découverte des irrationnels, créditée aux Pythagoriciens, et par les arguments de Zénon d'Elée.
b) Les absurdités rencontrées au XVIII^{e} siècle autour de l'analyse.
c) Les paradoxes de la théorie des ensembles avec Cantor.

Ces moments sont importants, car à chaque fois que les mathématiciens ont perdu foi en leur intuition, les réactions qu'ils eurent servirent à restructurer les mathématiques et à les acheminer progressivement à la forme qu'elles adoptent maintenant.

Premiers pas.

Les civilisations précédant les Grecs, comme celles des Balyloniens, des Chinois ou des Egyptiens (-3000 à -1000 environ), développèrent les mathématiques avant tout pour des besoins concrets, bien que de nombreux exemples contraires apparaissent en particulier chez les Balyloniens. Pour cette raison peut-être, la notion de preuve n'est jamais explicitée ou exhibée comme une valeur en soi. Au contraire, on nous présente des recettes. La géométrie est faite d'approximations suffisantes aux besoins; les méthodes sont très près du concret, de la manipulation et du tâtonnement. Le langage est en conséquence. On observe un tâtonnement systématisé très intéressant pour ceux qui recherchent la génèse des méthodes mathématiques.

a) En -1800, on trouve l'équivalent du problème suivant chez les Egyptiens:

$$x + \tfrac{1}{7}x = 21$$

le scribe fait une première tentative en posant $x = 7$. Sa

somme, au lieu de 21, donne 8. Il lui faudra donc multiplier son premier essai par autant de fois qu'il y a 8 dans 21. Il divise alors 21 par 8, par la méthode de "médiation" méthode qui a traversé les siècles jusqu'au Moyen-Age:

1	8
2	16 ✓
½	4 ✓
¼	2
1/8	1 ✓

Réponse: $2 + \frac{1}{2} + 1/8$

Ainsi, la réponse cherchée est 7 $(2 + \frac{1}{2} + 1/8)$

b) on assiste à un phénomène semblable de tâtonnement dans leur méthode primitive de multiplication (duplication):

17	x	12
1		17
2		34
✓ 4		68
✓ 8		136

Réponse: $68 + 136 = 204$

c) Les Balyloniens (-1700) avaient une méthode de tâtonnement plus sophistiquée débouchant sur une méthode générale pour résoudre certains types de systèmes d'équations:

à résoudre:

$$x + y = 2h$$
$$xy = p$$

ils posent $x = h + w$ où h est la demie-somme et w une correction; donc $y = h - w$

et alors $P = xy = (h + w)(h - w) = h^2 - w^2$

ainsi $w = \sqrt{h^2 - P}$

Les mathématiques grecques avec Pythagore et Zénon

Avec l'arrivée des Grecs (Thalès: -700), nous assistons à l'apparition de l'idée de preuve, la plus courte possible, des mathématiques étudiées pour elles-mêmes (preuves d'évidences), de critères esthétiques (beauté d'une preuve, instruments "euclidiens", etc.), du mépris des besoins pratiques, du besoin de rigueur (définitions, axiomes, lois de la logique), d'un langage précis, de l'abstraction (encore faible), d'un début d'axiomatisation, et d'un grand souci de la vérité.

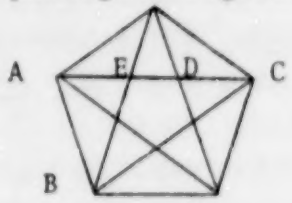
Ces préoccupations peuvent s'expliquer par des considérations diverses: économiques, politiques, sociologiques ou ethniques.

Alors que les mathématiques grecques progressaient à grands pas, tant arithmétiques que géométriques (mais surtout géométriques), une grave crise apparut avec la découverte des irrationnels chez les Pythagoriciens et les paradoxes de Zénon. Ce fut une crise de l'intuition. Il faut comprendre que l'intuition est une faculté qui est dépendante d'une époque. Le nombre rationnel, objet de notre intuition aujourd'hui, ne faisait pas partie du baggage intuitif de l'homme de Néanderthal. Le même phénomène se produisit chez les Grecs autour des concepts de nombre irrationnel et de limite (ou infini).

A) Pythagore (-585, -500), ou l'un de ses disciples, découvrit que la diagonale d'un carré de côté 1 ne pouvait s'exprimer comme un rapport de nombres (entiers), ou, en

d'autres mots, qu'il n'existait pas de nombre connu pouvant mesurer cette diagonale. (On trouve la preuve classique de ce fait chez Aristote (384 - 322) inspirée ou tirée des résultats des Pythagoriciens). Ceci venait bouleverser leur conception de l'univers. Leur intuition du monde, pour eux explicable par le nombre ou le rapport de nombres, était mise en défaut.

Certains disent que le premier irrationnel découvert, aussi par les Pythagoriciens, fut le nombre d'or qui apparaît comme un rapport de droites apparaissant dans leur signe de reconnaissance: le pentagone régulier.



En effet, le rapport $\frac{AC}{AD}$ (= $\frac{AC}{AD}$) se retrouve un très grand nombre de fois dans ce pentagone; ou même dans le pentagone intérieur délimité par les diagonales du premier. On constate que

$$\frac{AC}{AD} = \frac{AD}{AE}$$

Ce nombre est irrationnel. Si, en effet, on pose $\overline{AC} = 1$, $\overline{AD} = x$, $\frac{AC}{AD} = \frac{AD}{AE}$ devient $\frac{1}{x} = \frac{x}{1-x}$; c'est-à-dire $x^2 + x - 1 = 0$

et ainsi $x = \frac{-1 \pm \sqrt{5}}{2}$

Quoiqu'il en soit, le fond du problème est le même: c'est celui du continu, car on ne peut plus se fonder sur une unité fixée pour mesurer ces longueurs.

B) Zénon d'Elée (vers -450), veut défendre les vues de son maître Parménide qui soutient que le mouvement et le changement sont impossibles; il tente de détruire les deux vues exprimées par ses contemporains sur le mouvement, à savoir:

a) temps et espace se subdivisent à l'infini et donc le mouvement est continu;
b) le temps et l'espace sont constitués de petits intervalles et donc le mouvement est saccadé ou discret.

Il énonce 4 paradoxes, les deux premiers "contredisant" le point a), les deux autres "contredisant" le point b).

Il s'agit de 1. La dichotomie: objet qui ne peut partir puisqu'il doit effectuer une infinité de contacts en un temps fini.
2. Achille et la tortue: argument inverse de 1.
3. La flèche: au repos à chaque instant.
4. Le stade: rangées en mouvement où il faut imaginer un demi-intervalle de temps.

Le concept fondamental sous-jacent à ces paradoxes est celui de la limite (intimement relié à ceux de l'infini et de la continuité). Les Grecs avaient une mauvaise conception de la limite et de la convergence d'une série. Elle était uniquement géométrique. Ces paradoxes les firent se méfier de leur intuition arithmétique et ils se cantonnèrent dans la géométrie, terrain plus sûr, délaissant l'étude du mouvement, concept au centre de l'analyse. Ils rejetèrent par la même occasion l'infini arithmétique et géométrique. On le constate plus tard chez Euclide qui parle de longueurs.

que l'on peut prolonger aussi loin que l'on veut, mais jamais le terme infini n'apparaît. Il démontre qu'on peut toujours trouver un nombre premier plus grand que les précédents, mais il ne dit pas qu'il y en a une infinité.

Eudoxe (408-355)

Un règlement partiel de ces deux problèmes arrivera avec Eudoxe, l'un des grands mathématiciens grecs. Il sera l'un des initiateurs de la méthode axiomatique et provoquera l'orientation définitive des mathématiques grecques vers la géométrie. Par son approche, par ailleurs ingénieuse et remarquable, il fera dévier l'étude du problème du mouvement, brièvement posé, vers une mathématique statique.

a) Pour éviter les paradoxes de Zénon, il énonce un axiome, appelé par la suite Axiome d'Archimède, ou axiome de continuité, qui est le suivant:

Soient a et b, a < b, deux grandeurs; on peut alors ajouter a à lui-même un nombre suffisant de fois pour dépasser b.

C'est une façon, comme on le voit, d'éviter le problème des indivisibles contenus dans les paradoxes de Zénon et la question des limites. Ce sera le point de départ de la méthode d' "exhaustion" utilisée par Eudoxe lui-même pour démontrer que le volume d'un cône est le tiers du volume du cylindre qui le circonscrit. Cette méthode est énoncée chez Euclide:

"Si d'une grandeur, on soustrait une partie pas moindre que sa moitié, et si du reste on soustrait une partie pas moindre que sa moitié, et si ce processus se poursuit, il restera à la fin une grandeur plus petite que toute grandeur préassignée du même type."

Ceci est l'équivalent de notre proposition moderne qui dit:

Si M est donné, ε préassigné, et $\frac{1}{2} \leq r < 1$, alors $\exists N > o$ tel que $M (1 - r)^n < \varepsilon \; \forall n > N$.

ou encore

$$\lim_{n \to \infty} M (1 - r)^n = o$$

Archimède réutilisera cette affirmation pour découvrir des aires et des volumes.

b) Pour parer aux irrationnels, Eudoxe créera une arithmétique des grandeurs, (ce qu'on appelle aujourd'hui théorie des proportions) ou grandeur n'aura pas de signification pré-établie et pourra s'appliquer tout autant à une grandeur géométrique qu'à une grandeur arithmétique. Sa façon de procéder sera <u>axiomatique</u>, et son inspiration sera d'ordre géométrique. Cela constituera, à toutes fins pratiques, l'abandon de l'arithmétique et de l'algèbre. Il est significatif de trouver chez Euclide un volume des "éléments" entièrement consacré à la résolution de certaines équations algébriques par des méthodes purement géométriques.

Platon (430-349) et Aristote (384-322)

Ces deux philosophes grecs entérineront les méthodes de Eudoxe en tentant de les systématiser. C'est le début de l'étude des fondements des mathématiques et l'établissement définitif de la méthode axiomatique.

Platon le dit explicitement:

"Les nombres pairs et impairs, les figures et les trois sortes d'angles sont des hypothèses qu'on prend pour axiomes, qu'on ne discute pas, mais qu'on utilise pour arriver de façon consistante à des conclusions."

Platon voit dans la logique l'instrument des mathématiques. Il distingue entre concret et mathématiques (cf. l'allégorie de la caverne). Pour lui, les concepts sont découverts et non créés (VERITE MATHEMATIQUE). Il insiste sur le développement déductif des mathématiques et systématise les règles de la démonstration rigoureuse (diverses méthodes de preuve et en particulier preuve par absurde). Enfin, pour lui, le but de la science est de découvrir la structure de la nature et de l'articuler dans un système déductif. Cette vue, comme celle de Aristote qui la prolongera, aura d'ailleurs des répercussions néfastes sur le développement de la science jusqu'à la Renaissance.

Aristote, pour sa part, est encore plus précis. Il définit la définition et donne les conditions auxquelles elle doit répondre pour être valide. Il insiste sur la nécessité de termes non définis comme points de départ (idée qui sera perdue jusqu'au XIX^{e} siècle). Il distingue entre axiomes (lois de la logique) et postulats (valables pour une science

donnée), entre infini potentiel et infini actuel (qu'il rejette). Enfin, il fonde la science de la logique en distinguant quatorze types de syllogismes (ramenés aujourd'hui à 5).

On constate que depuis Pythagore, le fossé se creuse entre concret et abstrait, entre théorie et pratique. Il faudra attendre Archimède pour refaire temporairement le pont. Mais déjà, les mathématiques sont engagées dans un cul-de-sac.

Euclide (vers -300)

Euclide est celui qui vient synthétiser et ordonner dans une forme déjà acceptée et valorisée l'ensemble des connaissances mathématiques de ses prédécesseurs. Ses "éléments" constituent une histoire organisée. L'influence de ce livre sera énorme sur la pensée scientifique et mathématique occidentale. Ils constituent un résumé des "mathématiques élémentaires" du temps. C'est un modèle de rigueur jusqu'au XIX^{e} siècle, bien que criticable à plusieurs points de vue aujourd'hui. Ainsi, il "définit" ses termes primitifs et utilise maintes fois des postulats non énoncés. Il a un souci constant de la preuve la plus courte possible.

Ses "éléments" sont divisés en 13 chapitres:

- les 6 premiers traitent de géométrie élémentaire, y compris des problèmes d'algèbre traités géométriquement.
- les 3 suivants portent sur la théorie des nombres.
- le 10^{e} classifie les incommensurables.
- les 3 derniers étudient la géométrie spatiale, et surtout les polyèdres réguliers convexes.

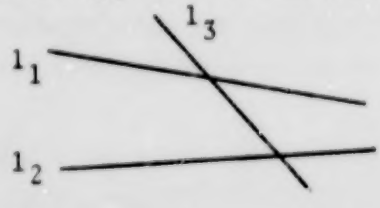
Le 1er livre comporte 23 définitions (point, ligne, surface, etc.), 5 postulats (axiomes) et 5 notions communes (logique).

Pour plus de détails, cf. Kline p. 58 et sq. .

Un point important sur les définitions, c'est qu'elles sont énoncées en termes d'autres mots non définis et que ces autres mots réfèrent à des concepts physiques. Ainsi, Euclide ne s'abstrait pas vraiment du concret. Il est à remarquer aussi que, pour Euclide, une ligne n'est jamais infinie.

Sur la véracité des postulats ou axiomes, les Grecs avaient peut-être une vue plus large que celle qu'on leur prête. Quoi qu'il en soit, les mathématiques postérieures prendront ces axiomes comme des dogmes de véracité et non de validité.

Le 5^{e} postulat énoncé par Euclide aura une importance toute particulière puisque les nombreuses tentatives pour le démontrer aboutiront à la création des géométries non-euclidiennes au milieu du XIX^{e} siècle. Euclide lui-même semble avoir tenté de le prouver (hypothèse fondée sur l'endroit où il le place dans ses "Eléments"), et de l'avoir posé comme postulat en désespoir de cause. Sa formulation, équivalente à la nôtre (par un point pris hors d'une droite, il ne passe qu'une et une seule parallèle), est la suivante:



Si l_3 vient couper deux droites l_1 et l_2, de sorte que la somme des angles intérieurs d'un même côté de la droite est plus petite que deux droits, alors l_1 et l_2 se rencontrent de ce côté si on les prolonge suffisamment.

Cette formulation semble originale à Euclide, et on lui doit le crédit d'en avoir vu la nécessité.

Brève libération de l'esprit axiomatisant: Archimède et Diophante

Archimède (287-212) était un homme pratique malgré qu'il s'en défendît. Il eut à résoudre des problèmes concrets et c'est probablement ce qui lui permit d'être plus souple face aux exigences logiques des Grecs. On lui doit une multitude de découvertes en divers domaines. Nous le mentionnons ici pour son apport au calcul intégral par le biais de la méthode d' "exhaustion" qu'il applique à plusieurs volumes, aires et longueurs de courbes. Il découvre ainsi les relations entre une sphère et le cylindre qui la circonscrit:

$$Vc = 3/2\ Vs$$
$$Sc = 3/2\ Ss$$

Pour des sections de coniques, il utilise des triangles:

Le tout est fondé sur le calcul de séries (progressions arithmétiques ou géométriques).

La faiblesse d'Archimède est de n'avoir pas développé de méthode générale d'intégration (calcul d'aires ou de volumes), faiblesse bien excusable vu le peu de connaissances sur les séries.

Diophante (vers +250), quant à lui, est l'un des rares mathématiciens grecs, à avoir étudié l'arithmétique et l'algèbre sans référence à la géométrie. Pour ce faire, il met au point un début de symbolisation algébrique. C'est pour ces deux raisons qu'il est quelquefois mentionné comme le père de l'algèbre.

Période allant de la fin des mathématiques grecques à Descartes

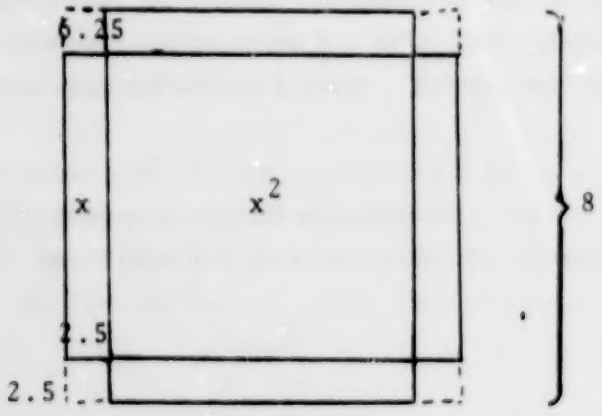
Cette période comprend les mathématiques indoues, arabes et occidentales du moyen-âge. Seule l'attitude face aux mathématiques nous intéresse ici. On assiste, avec les Indous (V^e au X^e siècle), à un renversement complet des valeurs mathématiques. La rigueur, l'axiomatique, la géométrie, l'esthétisme disparaissent pour faire place à l'intuition, aux "recettes", au mysticisme, à l'approximation, et surtout à un débloquage du côté de l'arithmétique et de l'algèbre. Les indous manupulent les nombres irrationnels, les nombres négatifs, et même l'infini ($^o/o$, $^a/o$) sans se poser de questions philosophiques, de sorte que ces nouveaux objets sont apprivoisés par leur manipulation courante. Pour les Indous, naturels, rationnels, négatifs, irrationnels obéissent sans problèmes aux mêmes lois algébriques. Cette période de manipulation naïve fut beaucoup plus féconde que l'attitude de défiance des Grecs, puisqu'elle permit de produire des résultats concrets immédiats et d'établir une banque de données nécessaires lors du développement logique de ces nouveaux êtres qui apparaîtront plus tard.

Les Arabes (VIII^{e} au XII^{e} siècle) reçurent le double héritage des Grecs et des Indous. D'esprit un peu plus critique que les Indous, ils commentèrent et approfondirent les textes grecs. Les méthodes indoues en arithmétique et algèbre leur paraissant moins fiables que celles de la géométrie, ils appuyèrent les unes sur les autres. En d'autres mots, la géométrie étant plus concrète que l'algèbre, ils vérifièrent les nouvelles lois de l'algèbre par la géométrie. Voici un exemple typique de ce fait que l'on trouve chez le plus célèbre des mathématiciens arabes, AL-KHOWARIZMI (825) dans son livre "Al-Jabr y muqabalah":

à résoudre $x^2 + 10x = 39$

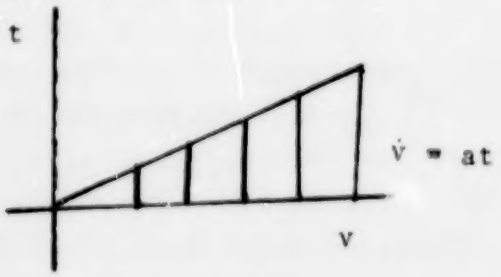
Après avoir trouvé la solution (la négative est écartée) algébriquement de façon assez voisine de la nôtre, il sent le besoin de vérifier géométriquement son résultat.

Il représente x^2 par un carré, divise 10x en 4 parties égales, 2.5x, qui deviennent des rectangles de côtés x et 2.5, complète le nouveau carré ainsi ébauché en ajoutant quatre carrés de côtés 2.5. Comme ceci a ajouté 25 au 39 déjà donné, il obtient un carré de surface 64 et donc de côté 8. Il en conclut donc que le x doit être 3. (8 - 2 x 2.5)



Etude du mouvement avec Oresure (1323-1382)

L'étude du mouvement avait été abandonnée depuis les paradoxes de Zénon. Les Indous et les Arabes ne l'avaient pas reprise. Au moyen-Age, cependant, les besoins se faisaient sentir avec le développement d'engins militaires, canons, catapultes, etc. . L'étude des corps tombants débutait. On discutait ferme cette question du mouvement et du changement dans les toutes nouvelles universités, du côté qualitatif plutôt que quantitatif. L'influence d'Aristote était encore toute puissante et l'on tentait de régler par le raisonnement les problèmes qui auraient dû être abordés par l'expérimentation. Oresme, évêque de Lisieux et professeur à Paris, est le premier à songer à représenter graphiquement la façon dont les choses varient, et à se rendre compte qu'une fonction à une inconnue peut se traduire par une courbe. Il a ainsi une première intuition de la géométrie analytique.



La figure ci-contre est sa façon de représenter le mouvement d'un corps ayant une vitesse uniformément accélérée. Il constate que la surface sous la courbe est l'espace parcouru.

Malheureusement, Oresme ne disposait pas d'une notation algébrique adéquate et ses travaux en resteront là jusqu'à Descartes.

Descartes et la géométrie analytique

L'idée d'allier géométrie et arithmétique (ou algèbre) n'était pas nouvelle au temps de Descartes (1596-1650). On peut remonter à Pythagore (nombres polygonaux, nombre d'or $\sqrt{2}$, etc.), passer par les Arabes (Al-Khowarizmi) et surtout par Oresme. Même Appolonnius, du temps d'Euclide, fit des tentatives de ce côté. Mais, avec Descartes, il ne s'agit plus seulement d'un parallèle, comme chez les Arabes, mais d'une véritable transcription en termes algébriques de phénomènes géométriques. Il fut aidé en cela par la nouvelle notation de Viète (1590) qui était une conséquence logique des nombreux et divers efforts, côté notation et symbolisation, observés chez les mathématiciens du XVI^{e} siècle.

Bien que ses fondateurs (Descartes et aussi Fermat (1601-1665)) ne l'aient pas remarqué, c'était là le début de l'arithmétisation de la géométrie et de l'unification des mathématiques. A nos yeux modernes, c'était aussi une "preuve" de la consistance de la géométrie en la ramenant à celle de l'arithmétique, bien qu'à cette époque, on ne mît pas en doute la géométrie. Ce fut également le début d'un essor considérable des mathématiques, car on pouvait dès lors formaliser la géométrie, la mécaniser en quelque sorte par les lois et méthodes de l'algèbre sans dépendre uniquement de l'intuition géométrique. C'est donc un retour à l'une des caractéristiques de la méthode axiomatique par un biais tout-à-fait inattendu.

Avec la géométrie analytique, s'ouvrira un vaste champs d'étude, celui du mouvement, du changement et de la variation, puisqu'elle devint aussitôt l'outil premier de l'analyse. On assistera alors à un ressourcement dans les sciences physiques.

Ce contact avec le monde physique développera une nouvelle confiance dans l'intuition, puisqu'il apparaît comme un modèle qui offre un terrain solide. Cette intuition s'avèrera pourtant un handicap au XVIII^{e} siècle lorsque de nouveaux paradoxes inhérents aux méthodes de l'analyse feront leur apparition.

Motivations pour l'apparition du calcul au XVIII^{e} siècle

4 types de problèmes pratiques se présentaient alors:

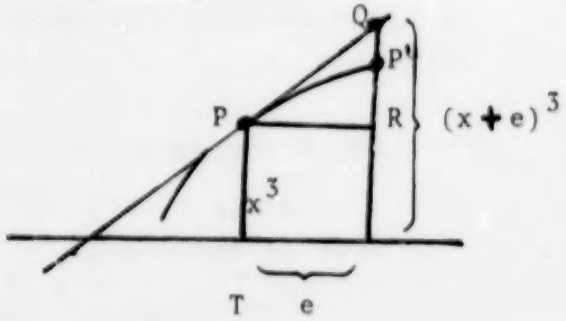
1) Calculer la vitesse de l'accélération, la hauteur, le point de chûte, etc., d'un bolide (Exemple: boulets de canon).
2) Trouver la tangente à une courbe:
   - -utile à l'optique
   - -utile pour connaître la direction de la vitesse d'un corps.
3) Trouver les maximum et minimum d'un fonction (canon).
4) Trouver des longueurs de courbes (planètes), des aires et des volumes.

Il ne fait pas de doute que c'est l'alliance de la dynamique et de la géométrie par le biais de la géométrie analytique qui est à l'origine du calcul. La tangente à une courbe, qui était chez les Grecs la courbe qui ne touche qu'en un seul peint, devient, au XVI^{e} siècle, avec Galilée, la direction de la vitesse d'un corps en ce point. Ce concept aura une grande importance dans le développement de l'analyse. Cette impureté première (relation à un concept physique) sera nécessaire. Ce n'est que plus tard qu'on rendra ce concept plus précis. (Ce sera alors la limite d'un rapport de variations).

Plusieurs mathématiciens européens s'attaqueront à ces problèmes (Cavalieri, Barrow, Fermat, etc.). Leurs efforts réunis créeront l'analyse. (Calcul différentiel et intégral). Voici, en guise d'introduction aux idées fondamentales de l'analyse, les approches de Fermat à ces problèmes.

a) Méthode de Fermat pour trouver la tangente à une courbe:

Soit la courbe de x^3



Si P' est très près de P, on peut pratiquement confondre P' et Q, de sorte que la pente de la tangente cherchée est

$\frac{P'R}{PR}$ c'est-à-dire $\frac{(x+e)^3 - x^3}{e} = x^3 + \frac{3x^2 \text{ et } 3xe^2+e^3 - x^3}{e} =$

$3x^2 + 3xe + e^2$

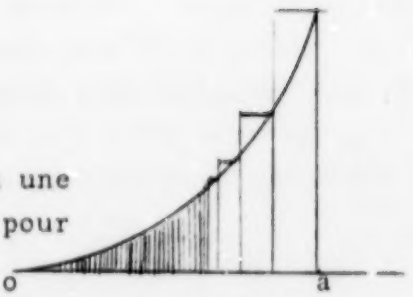
Fermat pose alors $e = o$, ce qui donne $3x^2$ (pente de la tangente en P).

b) Méthode de Fermat pour le calcul d'aire:

Soit $y = x^n$.

A chercher l'aire entre o et a.

Il subdivise l'intervalle (o, a) en une infinité de sous-intervalles en prenant pour abcisses: a, aE, aE^2, ... où $E < 1$.



Les aires successives des rectangles sont alors:

$$a^n (a - aE),\ a^n E^n (aE - aE^2),\ a^n E^{2n} (aE^2 - aE^3),\ \ldots$$

dont la somme est:

$$\frac{a^{n+1}(1 - E)}{1 - E^{n+1}} = \frac{a^{n+1}}{1 + E + E^2 + \ldots + E^n}$$

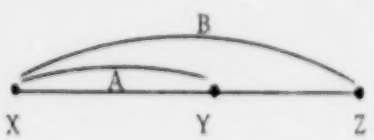
lorsque E tend vers 1, les rectangles deviennent extrêmement petits. Fermat pose alors $E = 1$; ce qui donne:

$$\frac{a^{n+1}}{n+1} = \text{aire sous la courbe entre o et a.}$$

Il prouve plus tard ce résultat pour $n \in \mathbb{Q}$.
Aujourd'hui, nous écrivons ce résultat $\int x^n dx = \frac{x^{n+1}}{n+1}$

c) Méthode de Fermat pour le calcul des maxima:

Le problème qu'il cherche à résoudre est celui de maximiser le produit $\overline{XY} \cdot \overline{YZ}$; il s'agit, en d'autres mots, de chercher l'aire maximale d'un rectangle à périmètre donné. Le résultat est fourni, comme on le sait, par un carré.



Fermat veut donc maximiser A (B - A), c'est-à-dire, $AB - A^2$. Il remplace A par A+E, l'autre partie est alors B - (A+E) et l'aire devient (A+E) (B - A - E).

Pour lui, E est une quantité très petite. Fermat émet alors l'hypothèse que près du maximum, la variation d'aire est presque nulle. C'est pourquoi, il pose

$$(A+E)\ (B - A - E) = AB - A^2$$

d'où : $EB = 2AE + E^2$

il divise par E: $B = 2A + E$

il pose E = o: $B = 2A$ ce qui donne un carré.

En termes plus modernes, sa démarche est presque la suivante:

$f(x)$ et $f(x+E)$ sont égaux en un maximum

$$\frac{f(x)}{E} = \frac{f(x+E)}{E}$$

c'est-à-dire: $\dfrac{f(x) - f(x+E)}{E} = o$

ce qu'on traduit aujourd'hui par

$$\lim_{E \to o} \frac{f(x) - f(x+E)}{E} = o \text{ ou } f'(x) = o.$$

On constate alors que malgré les lacunes logiques évidentes (diviser par E et poser E = o, alors que E est perçu au début comme une quantité positive fixe), son approche est essentiellement la nôtre, et comporte un caractère intuitif plus approprié à la didactique que notre procédé parfaitement rigoureux mais plus hermétique.

Newton (1642-1727) et Leibniz (1646-1716)

A l'arrivée de ces deux grands des mathématiques, les

principaux principes de l'analyse sont donc en place, dus à une pléiade de mathématiciens européens. En termes modernes, $\int x^n dx$ et $f'(x)$ font l'objet de procédés généraux qui ont déjà porté leurs fruits pour de nombreux problèmes pratiques. Mais c'est à Newton et Leibniz que l'on devra la découverte du lien entre ces deux concepts que sont l'aire sous une courbe et la tangente à cette courbe. Ce résultat que l'on nomme maintenant le théorème fondamental de l'analyse fut si important que l'on par le de Newton et Leibniz comme étant les fondateurs de l'analyse. La découverte est la suivante:

Concevons: "prendre l'aire sous une courbe"
et "chercher la tangente à une courbe"
comme des fonctions.

Alors ces fonctions sont inverses l'une de l'autre. Plus précisément, si $f(x)$ désigne la courbe en question:

$$\int f'(x)dx = f(x) + C \text{ où } C \text{ est une constante,}$$

et

$$\left[\int f(x)dx\right]' = f(x)$$

Mais l'ingéniosité de Newton et Leibniz ne se bornera pas à cette découverte. Tous deux verront l'utilité d'une méthode générale appliquée à toute courbe, et non seulement aux courbes polynomiales. Ils verront tous deux l'importance primordiale à accorder aux développements de fonctions en séries polynomiales infinies. En effet, si l'on sait "intégrer", c'est-à-dire, trouver l'aire, pour des polynômes, on le saura aussi pour toute fonction plus ou moins complexe, dès l'instant où on réussira à l'exprimer comme une série polynomiale. Ainsi, Newton et Leibniz utilisent des développements du type

$$\sin x = x - \frac{x^3}{3!} + \frac{x^5}{5!} - \ldots$$

$$\ln (1 \quad x) = x - \frac{x^2}{2} + \frac{x^3}{3} - \ldots$$

Ironiquement, c'est de cette nécessité de tels développements qu'origineront les troubles de l'analyse, puisqu'ils pré-supposent des notions claires de limite et de convergence inexistantes à l'époque. Chacun jouera à l'apprenti-sorcier avec ces séries et, curieusement, en tirera des conséquences pratiques extrêmement utiles.

Leibniz et la logique

L'arithmétique et l'algèbre par le biais de la géométrie analytique et de l'analyse sont devenues toute-puissantes au XVII^{e} siècle, éclipsant la géométrie pure et faisant passer inaperçue la découverte de la géométrie projective par Desargues. La tendance est à l'algébrisation des mathématiques. La logique n'y échappe pas lorsque ce génie "algébriste" qu'est Leibniz y touche. Avec son sens remarquable des opérations abstraites, Leibniz rêve de développer un langage universel qui puisse traduire toutes les pensées et raisonnements humains avec des règles (algébriques) si précises que l'on puisse décider mécaniquement si telle proposition est vraie ou fausse. Il ne réussira évidemment pas dans sa tâche, beaucoup trop complexe pour son époque. C'est en quelque sorte ce que réussira très partiellement Russell avec ses "Principia" en 1910. Ses tentatives l'amèneront cependant à algébriser la logique et à la conduire à la formulation mathématique qu'elle prendra plus tard. Il faut mentionner qu'à l'époque de Leibniz, la logique n'avait pratiquement pas progressé depuis les premiers essais d'Aristote, connus par sa classification des syllogismes et l'énoncé des règles de raisonnement. Le but premier de Leibniz fut donc de développer un langage mathématique qui permette au moins de formuler les syllogismes d'Aristote, ce qu'il réussit sans peine.

Il utilise symboliquement les opérations arithmétiques + et ., la négation, 0 et 1.

X + Y désigne l'ensemble des éléments ayant la propriété des éléments de X ou de Y.

X . Y ..... de X et de Y.

A ⊂ B désigne tout A est B.

X - Y désigne les éléments de X qui n'ont pas la propriété des éléments de Y.

1 désigne le vrai
o désigne le faux

Il reconnaît l'utilité d'étudier l'inclusion, les correspondances biunivoques (bijections). Il remarque au passage les surjections, les propriétés des relations d'équivalence.

Malheureusement, il arrive trop tôt et ses travaux seront oubliés jusqu'au XX^{e} siècle. C'est aux logiciens anglais, comme Boole, que reviendra l'honneur, au XIX^{e} siècle, de mettre véritablement sur pied la logique mathématique.

Lagrange, Canchy, Bolzanno, Weierstrass

Le XVIII^{e} siècle fut dominé par les développements de l'analyse devenue l'outil essentiel des sciences expérimentales. L'astronomie, la dynamique, la mécanique, l'optique lui doivent leurs fondements scientifiques. Du point de vue développement

théorique, on assiste à la mise en forme des principaux théorèmes de l'analyse (théorème de Rolle, règle de l'Hospital, séries de Taylor, théorème de la moyenne, etc.) et à la création de nouveaux champs d'étude reliés à l'analyse comme les séries infinies, les équations différentielles totales et partielles, la géométrie différentielle, etc.. Euler et la famille Bernouilli transcendent cette période. Les querelles autour des indivisibles, violentes au début du XVIII^{e} siècle, ne sont pas mortes, d'autant plus que le développement de l'analyse se fait dans des conditions quelque peu anarchiques et produit périodiquement des "paradoxes". Le manque de rigueur devient si grand que, malgré les résultats pratiques que fournit l'analyse, le "scandale" éclate et plusieurs mathématiciens, Lagrange (1736-1813) en tête, sentent le besoin urgent de remettre en question les bases mêmes de l'analyse vers les années 1770. Commence alors une période de restructuration qui, avec principalement Canchy (1789-1857), Bolzanno (1781-1848) et Weierstrass (1815-1897), aboutira à une formulation purement arithmétique vers 1850 des principaux concepts de l'analyse où l'intuition, trop souvent mauvaise conseillère, aura été pratiquement bannie.

Dès 1770, Lagrange a comme idéal d'écrire ses livres d'analyse et d'algèbre sans aucune référence à des figures ou à des raisonnements intuitifs. Il sera suivi en cela par ses successeurs. La confiance en l'arithmétique et l'algèbre va grandissante et surpasse celle que l'on arborait envers la géométrie. Cette confiance ne se manifestera pas seulement dans le traitement de l'analyse, mais dans presque toutes les branches étudiées au XIX^{e} siècle, comme la logique, les géométries, les probabilités. L'arithmétisation gagnera les mathématiques, et il n'est alors pas surprenant de voir les mathématiciens se pencher dans la deuxième moitié du siècle

sur les fondements des nombres (en particulier les réels), puisqu'une bonne partie de l'édifice repose dès lors sur ceux-ci.

Cette période (1770-1870) est ainsi caractérisée, suite aux déboires constatés en analyse, par un souci de rigueur nouveau et souvent extrême, par un mouvement vers l'arithmétique comme fondement des mathématiques, par un souci d'unification et un retour à une axiomatique renouvelée (comme nous le constaterons plus loin).

Après des tentatives, entre autres de Canchy, empreintes de trop d'intuition pour définir le concept central de la limite, Weierstrass la formalise dans sa forme actuelle, en des termes uniquement arithmétiques:

$$\lim_{x \to a} f(x) = b \qquad \text{si}$$

$\forall \varepsilon > 0, \exists \delta > 0$ tels que $|f(x) - b| < \varepsilon$ dès que $|x - a| < \delta$.

S'ensuivent les autres concepts de continuité et dérivée:

f est continue en a si $\lim_{x \to a} f(x) = f(a)$

$$f'(x) = \lim_{h \to 0} \frac{f(x+h) - f(x)}{h} \text{ si elle existe.}$$

Le concept même de fonction évoluera. Dirichlet (1805-1859) en 1837 la définira comme étant une loi faisant correspondre deux variables. Nous sommes déjà loin de l'idée que s'en faisait Descartes pour qui seules les fonctions définissables en termes des 4 opérations arithmétiques existaient.

Weierstrass "arithmétisera" ce concept en définissant la fonction comme un ensemble de nombres auquel correspond un autre ensemble de nombres. Les fonctions étaient encore restreintes chez lui aux fonctions de nombres. Il faudra attendre les travaux de Cantor et de ses successeurs pour trouver le concept moderne de fonction définie comme un ensemble particulier de couples d'un produit cartésien.

Lagrange, Galois, Grassmann, Cayley

Un pas de plus vers l'abstraction, l'axiomatisation et l'unification des mathématiques est accompli avec l'apparition du concept de groupe. On peut sans crainte placer ce concept à l'origine de l'algèbre moderne. Bien que la plupart des lois de groupe aient été reconnues avant Lagrange, la structure complète apparaît soudainement chez ce dernier sans signes précurseurs lors de son analyse de la résolution des équations en 1770.

Le problème central de l'algèbre jusqu'au XIX^{e} siècle demeurera celui de découvrir des formules générales pour exprimer rationnellement (c'est-à-dire à l'aide des quatre opérations élémentaires et de l'extraction de racines) les racines de polynomes. Les degrés 1 et 2 étaient réglés depuis les Babyloniens; les degrés 3 et 4 le seront en Italie au XVI^{e} siècle par Cardan et Ferrari (1545). Les degrés 5 et supérieurs demeureront une énigme jusqu'à Abel (1802-1829) et Galois (1811-1832). C'est en cherchant à résoudre ce problème que Lagrange observa le comportement de certaines fonctions ayant les racines d'un polynome comme variables. Les valeurs de ces fonctions ne changeaient pas, sauf quant au signe, lorsqu'il effectuait des permutations de ces variables.

Il remarqua alors que ces permutations obéissaient à certaines lois et découvrit même que certains sous-ensembles obéissaient aux mêmes lois et comportaient un nombre d'éléments diviseur du nombre total. Ce résultat (généralisé plus tard) porte aujourd'hui le nom de THEOREME DE LAGRANGE.

En 1799, Ruffini montre que la réciproque du théorème de Lagrange est fausse, à savoir que pour un diviseur du nombre total de permutations, il n'existe pas nécessairement un sous-ensemble obéissant à ces lois. Canchy aussi publie en 1815 quelques remarques sur les groupes de permutations. Mais c'est vraiment à Galois que l'on doit le pas décisif dans ce domaine. Le terme groupe lui appartient et il l'utilise dans un contexte beaucoup moins restrictif, tout en s'attaquant au même problème. Galois travaille à un tout autre niveau d'abstraction. Il reconnaît l'importance d'une autre structure, celle de corps de nombres. Voici, par un exemple, son approche.

Soit le polynôme $f(x) = x^2 - 2$. Sur $\mathbb{Q}$, ce polynôme n'a pas de racines. Dans $\mathbb{R}$, cependant, il possède deux racines: $\sqrt{2}$ et $-\sqrt{2}$. Si l'on adjoint ces deux nombres à $\mathbb{Q}$, et que l'on considère $\mathbb{Q}'$ le corps engendré, ce corps sera le plus petit corps contenant $\mathbb{Q}$ où $f(x)$ sera décomposable en $(x - \sqrt{2})(x + \sqrt{2})$. Galois le nomme corps de décomposition de $f(x)$. Il associe ensuite à $f(x)$ le groupe suivant (appelé par la suite groupe de Galois associé à $f(x)$):

$$G = \{h: \mathbb{Q}' \longrightarrow \mathbb{Q}' \mid h \text{ est un automorphisme et } h(x) = x \; \forall x \in \mathbb{Q}\}$$

Il détermine ensuite les conditions que doit remplir ce groupe pour que l'équation soit résoluble par radicaux.

Canchy, entre 1840 et 1860 publiera de nombreux articles sur les groupes, et Cayley en 1854 formulera la définition d'un

groupe abstrait dans des termes voisins de ceux d'aujourd'hui. Il énoncera notamment le théorème qui porte son nom, à savoir que tout groupe fini est isomorphe à un groupe de permutations. On continuera cependant à étudier principalement les groupes de permutations. Ainsi, en 1870, Jordan publie un "Traité des substitutions" couvrant ses propres résultats et ceux de ses prédécesseurs.

C'est vers cette époque aussi que l'on prend conscience du caractère unificateur de la notion de groupe, en arithmétique et en géométrie notamment. Grassman (1809-1877) publie en 1844 ses premiers résultats concernant les espaces vectoriels et les algèbres, applicables en géométrie analytique tri-dimensionnelle. Ses travaux englobent de façon très générale les notions de groupe et de corps. Hamilton cherche des corps de nombres englobant celui des nombres complexes et découvre les quaternions (1843). Boole (1815-1864) applique la notion générale d'opération à la logique (1847) et fait prendre conscience de son caractère abstrait et axiomatique. Gauss (1777-1855) développe en 1820 la théorie des congurences (entiers modulo) qui sera plus tard intégrée à la théorie des groupes. Enfin Klein (1849-1925) en 1872 dans son "Erlanger Programm" montre comment le concept de groupe peut unifier plusieurs branches des mathématiques. Il l'applique à la géométrie, qui a fait peu de temps auparavant un bond considérable avec la découverte des géométries non-euclidiennes, en montrant que les diverses géométries sont reliées entre elles par les groupes de transformations.

Parallèlement, la notion d'opération devient plus abstraite. Les lois arithmétiques, comme l'associativité ou la commutativité, perdent leur caractère de VERACITE, à mesure qu'on les applique à d'autres systèmes, pour acquérir plutôt un caractère de validité ou de cohérence. Ces lois s'insèrent graduellement dans un cadre axiomatique. Ainsi, Grassmann s'attaque à l'associativité, Hamilton à la commutativité, Boole à l'idempotence ($x + x = x$).

Géométries non-euclidiennes

Le facteur le plus marquant pour le changement dans la conception des mathématiques fut sans nul doute la découverte des géométries non-euclidiennes. Ce n'est pas un hasard si peu de temps après cette découverte on assiste à une poussée considérable de l'abstraction et de l'axiomatisation et à l'éclatement de la notion de vérité. La conception grecque des mathématiques refait surface, quoique transformée. La notion d'axiome réapparaît en force en prenant un nouveau sens.

On prend alors conscience que les mathématiques peuvent avoir autant pour but l'étude des liens entre les objets que les objets eux-mêmes et qu'elles peuvent ainsi se développer indépendamment du concret. L'application au monde réel n'est plus un critère.

Une toute nouvelle branche mathématique se greffe à cette découverte, celle de la métamathématique englobant la critique de la méthode axiomatique. En effet, la notion de vérité devenant relative, il faut la remplacer par celle de cohérence ou consistance.

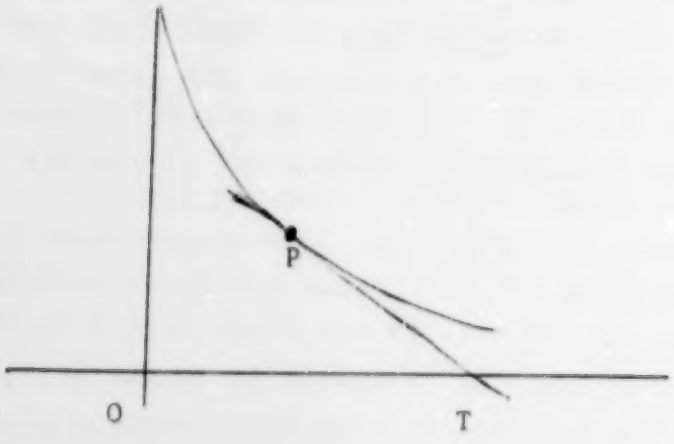
On se souvient que Euclide, dans ses Eléments, avait énoncé un postulat, le 5^{e}, équivalent à l'affirmation que d'un point pris hors d'une droite, il existe une et une seule droite parallèle à cette dernière. Ce postulat a fait l'objet d'un nombre incalculable de tentatives de démonstrations jusqu'au XIX^{e} siècle. On en doit plusieurs aux Arabes, notamment. Chaque fois, on utilisait implicitement et sans s'en rendre compte un postulat équivalent. Pratiquement tous les grands mathématiciens se sont attaqués à ce problème. Vers la fin du XVIII^{e} siècle, certains commencent à douter de l'inexistance d'une telle preuve. Une démarche alors naturelle est de prendre la négation de ce postulat comme axiome et de développer la géométrie en espérant découvrir des absurdités. Saccheri en 1733, Lambert en 1788 et Legendre en 1794 adoptent cette stratégie et découvrent effectivement des "absurdités" qui sont aujourd'hui des résultats classiques des géométries non-euclidiennes. Ils ne poussent cependant pas leur logique jusqu'au bout.

C'est à Gauss, Bolay (1802-1860) (Hongrois) et Lobachevsky (1793-1856) (Russe) que reviendra l'honneur de découvrir ces nouvelles géométries. Ce sont les premiers à pressentir que ce postulat était indémontrable à partir des autres. Gauss n'ayant rien publié sur le sujet (on a retracé sa découverte dans des notes personnelles), Bolay et Lobachevsky en eurent le crédit. Il est intéressant de remarquer que cette découverte se fit de façon indépendante chez chacun d'eux, comme cela s'est produit fréquemment dans l'histoire. La "génération spontanée" est plutôt rare en mathématiques! Tous trois ajoutent aux autres axiomes d'Euclide celui affirmant que d'un point pris hors d'une droite il existe plus d'une droite parallèle à cette dernière. Les théorèmes s'écartent alors rapidement des résultats classiques. Le plus célèbre affirme que la

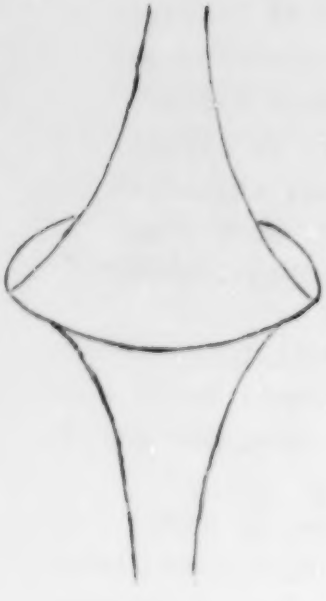
somme des angles intérieurs d'un triangle est inférieure à deux droits. Le tout est logiquement co-nstruit et ne comporte aucun paradoxe. On assiste à la même démarche chez Riemann qui, pour sa part, retient l'axiome affirmant que d'un point pris hors d'une droite, il n'existe aucune parallèle à cette dernière. Dans cette autre géométrie, la somme des angles intérieurs d'un triangle est supérieure à deux droits.

Un malaise demeure cependant: comment être sûr que le développement de ces nouvelles géométries n'aboutira pas un jour à des contradictions logiques dues à des contradictions premières entre les axiomes? C'est ce qu'on désigne aujourd'hui sous le nom de consistance d'un système axiomatique. Le plus sûr moyen, lorsqu'il existe, de répondre à cette question est de trouver un modèle, c'est-à-dire un ensemble où ces axiomes se vérifient, dans un domaine mieux connu où notre intuition peut nous guider. Ce type de problème s'est posé à maintes reprises au cours de l'histoire. Ainsi, le nombre négatif, rencontré comme un sous-produit des résolutions d'équations quadratiques, n'a acquis vraiment droit de cité que lorsqu'on a pu l'interpréter comme une dette ou une perte. Le nombre complexe a connu le même sort lorsqu'on l'a interprété comme un couple de points dans le plan cartésien. On n'a vraiment cru dans les géométries non-euclidiennes que lorsqu'on eut trouvé des modèles dans la géométrie euclidienne, domaine considéré comme plus sûr. Tout comme le plan est un modèle pour la géométrie euclidienne, la sphère le sera pour la géométrie de Riemann, et la pseudo-sphère pour la géométrie de Bolay et Lobachevsky. Ces modèles sont respectivement de courbure nulle, positive et négative.

La pseudo-sphère est un volume de révolution engendré par la "tractrice", courbe dont le rapport PT à OT est constant (PT = tangente en P)



La pseudo-sphère a l'allure suivante



Dans chacun de ces modèles, on constate que la définition de distance est celle de géodésique, c'est-à-dire le plus court chemin entre deux points tout en demeurant sur la surface. On peut même dire que la notion de distance détermine la géométrie. Riemann va plus loin en imaginant des surfaces où la notion de distance varie en chaque point créant ainsi une multitude de nouvelles géométries.

Gauss, face à cette découverte, avait perdu confiance en la géométrie et affirmait que la vérité (entendre: la consistance) devait être recherchée dans l'arithmétique. C'était, comme on l'a vu, la tendance générale dans les autres branches. Les géométries non-euclidiennes reposant sur la géométrie euclidienne, on cherchera plus tard à faire reposer cette dernière

sur l'arithmétique. Grassmann y parviendra indirectement avec les espaces vectoriels; Hilbert le fera de façon explicite en 1899. Mais même l'arithmétique n'apparaîtra pas assez sûre aux mathématiciens et Frege en 1903 fera reposer l'arithmétique sur les ensembles, lesquels reposeront sur la logique avec Russell.

Boole, Venn, Carrol

La logique mathématique, ou le besoin de fonder sur des bases mathématiques les principales lois de la pensée, avait peu progressé depuis Aristote. Seul Leibniz avait fait une tentative prometteuse mais qui avait tourné court. Le regain de popularité envers l'arithmétique comme fondement de l'analyse n'est peut-être pas étranger à la réanimation de la logique formelle au milieu du XIX^{e} siècle. C'est l'Angleterre qui fournira les précurseurs en ce domaine. Dans l'ombre depuis les querelles autour de l'analyse entre les tenants de Leibniz (continental) et Newton (Anglais), les mathématiques anglaises reviendront en force avec George Boole (1815-1864), John Venn (1834-1923), Auguste De Morgan (1806-1871) et même Lewis Carroll (Charles Dodgson) (1832-1898).

En 1847, Boole publie:

"The mathematical Analysis of logic - Being an essay towards a calculus of Deductive Reasoning".

Le but de Boole est de systématiser les lois de la logique en utilisant le langage et les méthodes de l'algèbre, le tout dans un cadre axiomatique. Il pose donc un certain nombre d'axiomes, qui sont en réalité certaines lois élémentaires du raisonnement mises en forme algébrique, et en tire une série de

théorèmes. Il crée ainsi ce qu'on appelle aujourd'hui l'algèbre de Boole, ou encore les treillis.

Il dénotait par x, y, z, ... les classes d'objets ou d'idées par X, Y, Z, ... les éléments de ces classes. 1 désignait la classe universelle, 0 la classe vide. xy signifiait l'intersection de x et y, x + y la réunion disjointe. Le complément de x est noté 1 - x, et plus généralement x - y désigne la classe des éléments de x qui ne sont dans y. xy = x remplace notre écriture: $x \subset y$.

Quelques axiomes:

$x(1 - x) = 0$ Principe de contradiction

$xy = yx$

$xx = x$

$x + y = y + x$

$x(u + v) = xu + xv$

$x + (1 - x) = 1$ tiers exclus.

Boole remarque aussi que son calcul "booléen" peut aussi s'appliquer au calcul propositionnel où

x = 1 signifierait que x est vraie,
x = 0 que x est fausse,
1 - x désignant la négation de x.

Mais il ne pousse pas très loin cette étude. Boole peut ainsi être regardé comme le réformateur de la logique qui la détache du domaine de la philosophie et la rattache aux mathématiques.

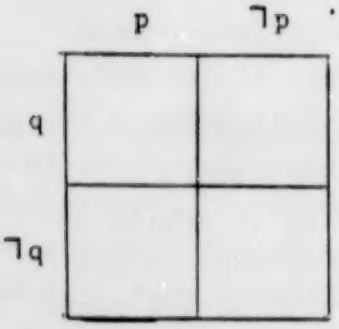
C'est Charles Peirce, américain (1809-1880) qui fera progresser le calcul propositionnel en distinguant entre proposition et forme propositionnelle et en introduisant des formes propositionnelles de plus d'une variable. Gottlob Frege (1848-1925)

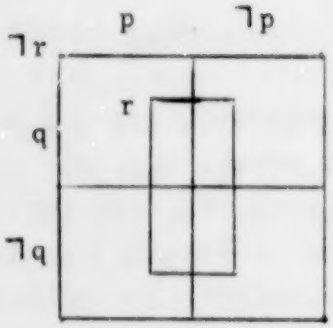
sera celui qui fera entrer la logique dans l'étude des fondements des mathématiques. Il introduit les quantificateurs, l'implication (selon la définition moderne), distingue entre x et {x}, entre $\in$ et $\subset$, axiomatise la logique, et tente de faire des mathématiques une extension de la logique. En 1884, les définitions et les opérations sur les nombres sont dérivés de la logique. Après les catastrophes apportées par la théorie des ensembles de Cantor, c'est à Bertrand Russell (1872-1970) que reviendra cette construction dans ses "Principia Mathematica" (1910-1913).

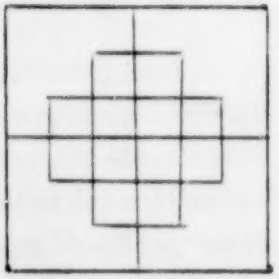
Brèves remarques sur Venn et Carroll

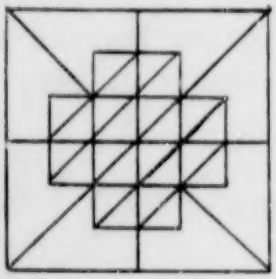
John Venn fut un logicien amateur peu important du point de vue théorique. Il décide cependant de représenter par des diagrammes les principes et lois logiques dans son ouvrage "Symbolic logic" publié en 1881. Il n'est pas le premier à vouloir utiliser de telles représentations puisque Euler au XVIII^{e} siècle et De Morgan avaient eu aussi cette idée, mais sans la développer, et sans la généralité de Venn.

Lewis Carroll, de son vrai nom Charles L. Dodgson, fut un professeur de mathématiques à l'Université d'Oxford. Il est l'auteur de plusieurs contes pour enfants dont "Alice au pays des merveilles". Il écrit ces livres, de même que des livres de didactique sur la logique symbolique, après s'être retiré de la vie universitaire vers 50 ans. Il émet une loi qui sera reprise par Russell lors de son axiomatisation de la logique, la loi du "MODUS PONENS", dans son ouvrage "logique sans peine". C'est dans ce même livre qu'il développe un système de représentation par diagrammes de syllogismes logiques. Notre utilisation actuelle est une variante de la sienne.







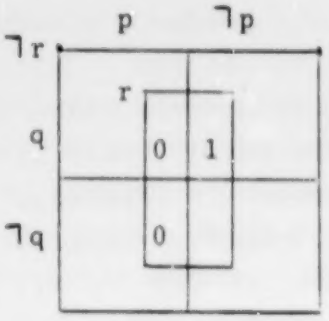


etc.

Il utilisait ces diagrammes pour tirer les conclusions de certaines prémisses d'un syllogisme ou vérifier la validité d'un syllogisme.

Exemple:

Aucun docteur n'est enthousiaste;
or, vous êtes enthousiaste;
donc, ...



Docteur: p
enthousiaste: r
vous: q

Cantor et la théorie des ensembles

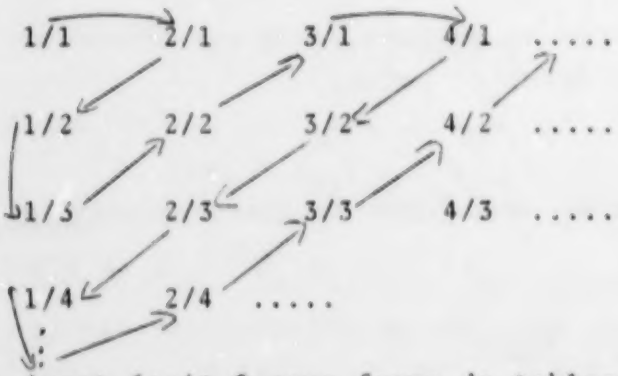
Georg Cantor (1845-1918) a été amené à développer la théorie des ensembles (infinis) par des problèmes qu'il a rencontrés en analyse lors de ses travaux sous la direction de Weierstrass relatifs aux développements des fonctions en séries de Fourier. Il étudiait les conditions pour qu'une fonction soit développable en une telle série, et ces conditions étaient reliées aux ensembles de points de discontinuité que comportait cette fonction. Ces ensembles étaient bien sûr des ensembles de nombres réels. Il s'agissait de déterminer la "grandeur" de ces ensembles infinis.

En 1872, il "définit" un ensemble:

> "Par ensemble, on entend un groupement en un tout d'objets bien distincts de notre intuition ou de notre pensée".

L'outil-clef pour comparer des ensembles sera la bijection ou correspondance biunivoque. Il n'est pas le premier à utiliser ce concept: Galilée s'en sert pour dire qu'il y a "autant" de nombres pairs que de nombres entiers; Leibniz le mentionne aussi. Mais il est le premier à l'utiliser systématiquement. Le "comptage" ne suffit plus lorsqu'il s'agit d'infini, et il faut suppléer à notre intuition par un concept mathématique précis. Il est essentiel cependant qu'il soit la continuation du cas fini, ce qui est le cas puisque deux ensembles finis ont même nombre d'éléments si et seulement si il existe une bijection entre eux. Ceci peut constituer la définition d'un ensemble fini, alors qu'un ensemble infini serait celui qui est en bijection avec un de ses sous-ensembles stricts. Dédekind a procédé ainsi dans les années 1880.

Muni de cet outil, Cantor compare dès 1872 $\mathbb{N}$ et $\mathbb{Q}$ pour constater qu'ils peuvent être mis en bijection. Il appelle ensemble dénombrable tout ensemble pouvant être mis en bijection avec $\mathbb{N}$. Deux ensembles en bijection sont appelés équipotents, ou de même puissance, ou de même cardinalité. Un ensemble dénombrable est un ensemble dont les éléments peuvent être disposés sousforme de suite. Pour $\mathbb{N}$ et $\mathbb{Q}$, il procède comme suit:



Ayant écrit $\mathbb{Q}$ sous forme de tableau à deux directions infinies, il indique la façon de disposer $\mathbb{Q}$ sous forme de suite et prouve par le fait même sa dénombrabilité.

A l'époque, on disposait de deux façons d'aborder les réels: d'abord, en les classifiant en rationnels et irrationnels, ensuite en nombres algébriques et nombres transcendants. Un nombre est algébrique s'il est racine d'un polynôme à coefficients rationnels; autrement, il est transcendant. $\sqrt{2}$ est algébrique puisqu'il est racine de $x^2 - 2$. Par contre, π et e sont transcendants. Ceci a été démontré en 1873 pour e et en 1882 pour π. Cantor démontre dès 1873 que l'ensemble des nombres réels algébriques est dénombrable et que l'union d'un nombre quelconque d'ensembles dénombrables est encore dénombrable. De là, l'importance du problème qu'il se pose aussitôt:

est-ce que $\bar{\bar{\mathbb{N}}} < \bar{\bar{\mathbb{R}}}$? Si oui, comme $\bar{\bar{\mathbb{R}}}$ = {nombres algébriques}$\cup$ {nombres transcendants}, l'ensemble des nombres transcendants ne peut être dénombrable. [Remarque: $\bar{\bar{\mathbb{N}}} < \bar{\bar{\mathbb{R}}}$ signifie qu'il n'existe pas de bijection de $\mathbb{N}$ à $\mathbb{R}$]. Ce résultat assurerait donc l'existence d'un "nombre considérable" de transcendants, en fait, "autant qu'il y a" de nombres réels! Il répond par l'affirmative à ce problème, en 1873, de la façon suivante:

Il procède par l'absurde et suppose que $\mathbb{R}$ est dénombrable; il peut s'écrire sous forme de suite,

$$\mathbb{R} = \{u, u_2, u_3, \ldots, u_n, \ldots\}.$$

Il écrit alors chaque u_i sous forme de développement décimal.

$$\begin{aligned} u_1 &= a_{11}a_{12}\cdots a_{1m}\cdots \\ u_2 &= a_{21}a_{22}\cdots a_{2m}\cdots \\ &\vdots \\ u_n &= a_{n1}a_{n2}\cdots a_{nm}\cdots \\ &\vdots \end{aligned}$$

Et il construit un nombre réel y qui n'apparaît pas dans cette suite

$$y = b_{11}\, b_{22} \cdots b_{nn} \cdots \text{ où } b_{ii} \neq a_{ii} \ \forall i$$

Ce nombre différant de u_i au moins en sa i^e décimale est alors distinct de tous les nombres de la suite. Contradiction.

Cantor a dès lors mis en évidence deux sortes d'infini, celui de $\mathbb{N}$ et celui de $\mathbb{R}$ qui ne peuvent être confondus. Y en a-t-il d'autres? Il cherche alors à comparer $\mathbb{R}$ et $\mathbb{R}^2$ espérant trouver un troisième type. A son grand étonnement, il décou-

vre en 1877 qu'ils ont même cardinal, c'est-à-dire qu'ils peuvent être mis en bijection. En réalité, il se limite à montrer que $\overline{[0, 1]} = \overline{[0, 1]^2}$, puisqu'il est facile de montrer que $\overline{\mathbb{R}} = \overline{[0, 1]}$ et que $\overline{\mathbb{R}^2} = \overline{[0, 1]^2}$. Il découvre même une preuve que $\overline{[0, 1]} = \overline{[0, 1]^n}$. Sa preuve est la suivante:

Soit $(x_1, \ldots, x_n) \in [0, 1]^n$. Ecrivons x_i en développement décimal.

$$x_1 = a_{11}a_{12}\cdots a_{1m}\cdots .$$
$$x_2 = a_{21}a_{22}\cdots a_{2m}\cdots .$$
$$\vdots$$
$$x_n = a_{n1}a_{n2}\cdots a_{nm}\cdots .$$

et posons

$$y = a_{11}a_{21}\cdots a_{n1}a_{12}a_{22}\cdots a_{n2}\cdots a_{1m}a_{2m}\cdots a_{nm}\cdots .$$

Il est alors facile de vérifier que la fonction

$$f(x_1, \ldots, x_n) = y \text{ est une bijection.}$$

(Remarque: il faut prendre la convention que, par exemple, $\frac{1}{2} = 0.4999.....$ et non $0.50... .$)

Peano, en 1890, donne une preuve remarquable que $\overline{[0, 1]} = \overline{[0, 1]^2}$:

Soit $x \in [0, 1]$. Ecrivons x en développement quaternaire:

$$x = a_1a_2\cdots a_n\cdots, \quad 0 \leq a_i < 3.$$

Divisons le carré en 4 parties égales. Si $a_1 = 0$, plaçons-nous dans le carré 1, si $a = 1$, dans le carré 2, etc..

Supposons que $a_1 = 2$; nous sommes alors dans le carré 3. Divisons le en 4. Regardons a_2 et procédons de la même façon

que pour a_1. Il est clair que nous allons ainsi aboutir à un point unique du carré. Associons x à ce point. Nous avons alors une bijection.

Cantor ne se décourage pas et découvre par le biais des ensembles bien ordonnés (qu'il nommera ordinaux) un moyen de construire des nombres cardinaux infinis de plus en plus grands qu'il appelle des alephs. En 1884, il découvre un moyen plus simple en démontrant que $\overline{A} < \overline{\mathcal{P}(A)} = 2^{\overline{A}}$.
Il peut ainsi bâtir la suite: $\overline{\mathbb{N}} < 2^{\overline{\mathbb{N}}} < 2^{2^{\overline{\mathbb{N}}}} < 2^{2^{2^{\overline{\mathbb{N}}}}}$, ...

Il écrit en 1884:

"Dieu tout-puissant a voulu que je parvienne aux lumières les plus étonnantes et les plus innattendues sur la théorie des ensembles et sur la théorie des nombres, ou, bien plus, que je trouve ce qui depuis bien des années a fermenté en moi, ce vers quoi j'ai fait de longues recherches".

Cantor, critiqué et ridiculisé par son entourage pour avoir osé s'attaquer au tabou de l'infini actuel, fait une dépression nerveuse entre 1884 et 1886. Jusqu'en 1897, il parfait sa théorie, mais termine sa vie dans un asile d'aliénés où il entre en 1897.

Vers 1896, il découvre une faille dans sa théorie: l'ensemble de tous les cardinaux ne peut exister, car son cardinal doit être à la fois dans cet ensemble et à la fois plus grand que chacun des éléments de cet ensemble. Même faille avec

l'ensemble des ordinaux. Il cherche alors à réparer la brèche en posant des conditions (débuts de l'axiomatisation) pour limiter l'apparition d'ensembles "trop grands". D'autres mathématiciens découvrent à la même époque d'autres paradoxes de sa théorie. En 1903, Russell envoie à Frege (qui venait de fonder l'arithmétique sur les ensembles dans un livre qui allait paraître) le paradoxe suivant:

Soit $S = \{\text{ensembles } x \mid x \notin x\}$
alors si $S \in S$, $S \notin S$ et si $S \notin S$ alors $S \in S$.

D'autres paradoxes feront leur apparition: antinomie de Richard, le mot hétérologique, le barbier qui fait la barbe à tous ceux qui ne se rasent pas, Epiménide le crétois, etc..

Cette fois, la réaction des mathématiciens face à ces paradoxes causés par l'intuition chancelante est plus complexe que celle des Grecs face à Zénon et aux irrationnels, ou que celle des mathématiciens du XVIII^{e} siècle face aux paradoxes de l'analyse. Il y a encore une fois la réaction axiomatisante. Zermelo en est le chef de file. Fraenkel, Bernays suivent. Leur approche est de limiter par des axiomes les ensembles paradoxaux.

D'autres mathématiciens s'insurgent contre ce procédé apparemment arbitraire et soutiennent que le fond du problème est du côté logique. Ils cherchent un commun dénominateur à tous ces paradoxes et concluent que dans chacun, on utilise le terme même à définir dans sa définition. Ainsi l'ensemble des ensembles qui ne se contiennent pas comme élément. Leur réaction est donc d'axiomatiser la logique et de bannir par des règles de formation de formules de telles définitions. Russell est l'homme qui fera ce travail de restructuration à partir de la logique. Les tenants de cette approche seront

appelés les logicistes. Mais lorsqu'il veut développer la théorie des ensembles à partir de la logique, Russell doit inventer un nouveau type d'objets pour parler de l'"ensemble" des ensembles: il parle alors de la classe des ensembles. Il doit inventer un nouveau type d'objets pour décrire les classes de classes. Et pour ne pas complexifier ainsi à l'infini, il pose un nouvel axiome sur ces nouveaux objets. Cet axiome paraît aussi arbitraire que les axiomes des tenants de l'axiomatique de la théorie des ensembles.

Enfin, certains autres mathématiciens, minoritaires, rejettent les deux approches précédentes. Ils mettent en doute certains principes logiques comme le tiers exclus qui est utilisé à satiété dans les preuves mathématiques pour prouver l'existence ou la non-existence d'êtres mathématiques sans donner un moyen explicite de les construire. Au nom de l'intuition, ils rejettent l'infini actuel et toute preuve non-constructive. Brouwer, Hollandais, en est le chef de file. Ils tentent encore aujourd'hui de reconstruire les mathématiques sur ces nouveaux principes. Malheureusement, la totalité des résultats trouvés avant le XX^{e} siècle n'est pas récupérable.

Nous avons hérité, dans l'enseignement actuel à l'élémentaire, de ces réactions: insistance sur la logique, sur la théorie des ensembles comme fondation des mathématiques, sur la "constructivité" ou concrétisation. Mais il s'agit véritablement d'un sous-produit dont les buts réels ont été perdus de vue. On peut se demander à la lumière de l'histoire, du bien-fondé de cette approche.

L'une de ces écoles ayant fait tout reposer sur la logique, eut comme principale influence de poser des questions d'ordre métamathématique importantes qui occuperont les logiciens pour de nombreuses années. Ainsi, quelle est la valeur

de l'axiomatisation? Nous redonne-t-elle tout ce qu'on voulait y mettre (complétude)? Nous assure-t-elle contre les contradictions (consistance)? Est-elle trop riche (indépendance)? Pouvons-nous atteindre par ces règles du raisonnement tout ce que l'intuition nous fait découvrir?

Gödel en 1931 apporte des réponses dramatiques à quelques-unes de ces questions. Voici schématiquement ses deux principaux résultats:

a) Il est impossible d'établir la preuve qu'un système axiomatique, assez riche pour y développer l'arithmétique (par exemple, l'axiomatique de la logique de Russell), soit consistant (c'est-à-dire exempt de contradictions).

b) Tout système axiomatique assez riche pour y développer l'arithmétique est essentiellement incomplet (c'est-à-dire, qu'il existera toujours des affirmations vraies mais indémontrables).

On assiste curieusement avec ces résultats à une revalorisation de l'intuition (ou de la pensée informelle) après ses maintes chûtes historiques!

Système axiomatique de Zermelo-Fraenkel.

1. Axiome d'extension

$\forall x, y\ (\forall z\ (z \in x \Longrightarrow z \in y) \Longrightarrow x = y)$

deux ensembles sont égaux sii ils ont les mêmes éléments.

2. Axiome de l'ensemble vide

$\exists x\ \forall y\ (\sim y \in x)$

3. Axiome des couples non ordonnés

$\forall x, y, \exists z\ \forall w\ (w \in z \Longleftrightarrow w = x \vee w = y)$

Si x et y sont des ensembles, alors la paire {x, y} est un ensemble.

4. Axiome de l'ensemble-somme ou union

$\forall x\ \exists y\ \forall z\ (z \in y \Longleftrightarrow \exists t\ (z \in t \ \& \ t \in x))$

Si x est un ensemble d'ensembles, l'union de ses membres est un ensemble.

5. Axiome de l'infini

$\exists x\ (\emptyset \in x \ \& \ \forall y\ (y \in x \Longrightarrow y \cup \{y\} \in x)$

6. Axiome de remplacement

$\forall t_1, \ldots, t_k\ (\forall x\ \exists! y\ A_n\ (x, y; t_1, \ldots, t_k) \Longrightarrow \forall u\ \exists v\ B\ (u, v)$

où $B\ (u, v) \equiv \forall r\ (r \in v \Longrightarrow \exists s \in u \ \& \ A_n\ (s, r; t_1, \ldots, t_k))$

Dit en gros que toute formule permise définit un ensemble, celui satisfaisant à la propriété exprimée par la formule.

7. Axiome de l'ensemble-puissance

$$\forall x \, \exists y \, \forall z \; (z \in y \Longrightarrow z \subseteq x)$$

8. Axiome du choix

9. Axiome de régularité

$$\forall x \, \exists y \; (x = \emptyset \vee (y \in x \; \& \; \forall z \; (z \in x \Longrightarrow \neg z \in y))$$

Prohibe: $x \in x$

Axiomatique de la logique élémentaire.

A. Axiomes

1. $p \vee p \Longrightarrow p$
2. $p \Longrightarrow (p \vee q)$
3. $p \vee q \Rightarrow q \vee p$
4. $(p \Rightarrow q) \Longrightarrow ((r \vee p) \Longrightarrow (r \vee q))$

B. Règles de formation de formules

a) p est une formule

b) Si $p \Longrightarrow q$ sont des formules, alors $p \Longrightarrow q$ est une formule.

c) Si $p \Longrightarrow q$ est une formule, $\sim (p \Rightarrow q)$ est une formule.

d) Si S_1 et S_2 sont des formules, $S_1 \vee S_2$ est une formule.

e) Si S_1 et S_2 sont des formules, $S_1 \wedge S_2$ est une formule.

C. Règles d'inférence ou de transformation

a) Règle de substitution:
Si une formule contient une variable propositionnelle, on peut la substituer partout par une formule.

b) Modus ponens:
Si S_1 et $S_1 \Longrightarrow S_2$ sont vraies, alors S_2 est vraie.

§2 Notion de structure, types et exemples

Le terme structure est vague. Il dénote un esprit plus qu'un concept. Il est relié étroitement à la méthode axiomatique et procède de la reconnaissance d'un "patron" logique s'appliquant à plusieurs situations en apparence dissemblables. L'unification des mathématiques est largement tributaire de ce concept. Considérons les paires de situations suivantes:

Les blocs logiques.	Le jeu des Personnages.
Les rotations autour d'un point.	Les nombres relatifs $\mathbb{Z}$.
Un treillis $(A, \sqcap, \sqcup)$.	Un circuit électrique.

Indépendamment de la nature des objets et de la nature des relations entre les objets, on perçoit une ressemblance entre ces situations prises deux à deux: elles sont "structurées" de façon semblable.

Le sens du mot structure variera selon ce que l'on considère l'essence d'une situation. Ainsi $\mathbb{Z}$ peut être vu comme un ensemble d'objets muni d'une relation, l'addition, et répondant à certaines lois (par exemple, l'associativité). Il peut être aussi vu comme un groupement (d'au moins deux façons), ou comme un ensemble de points équidistants sur une droite.

On peut aussi appliquer le mot structure à des situations plus vastes. Ainsi, toutes les mathématiques tournant autour de l'étude d'ensembles d'objets munis d'opérations concerneront les structures algébriques. Il s'agit ici d'un rapprochement beaucoup plus abstrait, englobant la méthodologie, le type de questions étudiées, etc..

On peut distinguer un certain nombre de telles grandes catégories:

structures algébriques,
structures géométriques,
structures logiques,
structures topologiques.

Cette liste n'est ni exhaustive ni bien déterminée. Ce qui intéresse le mathématicien dans cette vaste classification, c'est le rapprochement entre les formulations des systèmes d'axiomes. Ainsi, les axiomes des systèmes répondant aux structures algébriques suivent un certain "patron": il y a des objets, une ou des opérations, et les axiomes portent sur des propriétés de ces opérations. Les structures topologiques suivent un autre "patron": il y a des objets dans un univers (espace) et l'on s'intéresse à des "voisinages" des objets, c'est-à-dire à des sous-ensembles répondant à certaines conditions. Dans les structures logiques, il y a un "alphabet", des formules composées de cet alphabet, des règles de composition de "bonnes" formules, certaines formules prises comme axiomes, des règles de raisonnement ou d'inférence.

Ce qui caractérise le mot structure semble donc être ce qui rapproche certaines situations, ou certaines classes de situations, après avoir fait abstraction de certaines qualités (nature des objets, nature des relations ou opérations, etc).

1. Les groupes

La notion de groupe occupe une place centrale dans les mathématiques. Elle se retrouve dans la plupart des branches mathématiques. La notion d'opération en est la pierre angulaire.

Définition: Soit A un ensemble, une opération binaire sur A est une application du type:

$$A \times A \longrightarrow A.$$

On pourrait aussi définir opération n-aire ou opération partielle. Pour cette dernière, on exige alors fonction au lieu d'application.

Définition: Une structure de groupe est définie sur un ensemble G, si G est muni d'une opération, notée *, répondant aux axiomes suivants:

G1) $\forall a, b \in G \quad a * b \in G$ [Fermeture]

G2) $\forall a, b, c \in G, a * (b * c) = (a * b) * c$ [associativité]

G3) $\exists e \in G$ tel que $\forall a \in G \quad a * e = a = e * a$ [e = unité]

G4) $\forall a \in G, \exists a' \in G$ tel que $a * a' = e = a' * a$ [symétrique]

La commutativité n'est pas exigée. Si on ajoute

G5) $\forall a, b \in G \quad a * b = b * a,$

On définit alors un groupe commutatif ou abélien.

On développe généralement la théorie des groupes de façon axiomatique en prouvant certains faits découlant de ces seuls axiomes. Si l'on veut étudier une classe plus spéciale de situations, on ajoute certains axiomes et l'on poursuit.

Cette formulation axiomatique n'est pas unique. On peut vouloir ajouter des axiomes superflus pour faciliter les preuves, ou les réduire au minimum pour des raisons esthétiques. La formulation ci-haut est essentiellement celle due à Cayley vers les années 1860.

Exemples de groupes

$\langle \mathbb{Z}, + \rangle$, $\langle \mathbb{Q}, + \rangle$, $\langle \mathbb{Q}^*, \times \rangle$, $\langle$rotations, $\circ$, $\langle$transformations affines, $\circ$

$\langle$permutations de n objets, $\circ$, $\langle$bijections de A dans A, $\circ$, $\langle$mouvements d'une figure géométrique plane ou solide, $\circ$

$\langle$racines $n^{\text{ièmes}}$ de l'unité, $\times$, $\langle$entiers modulo n, $+$, $\langle \mathbb{Z}_p, \times$, $\langle$polynomes sur $\mathbb{Q}$, $+$

$\langle$matrices sur $\mathbb{R}$, $+$, $\langle$quaternions*, $\times$, $\langle$translations, $\circ$

$\langle$homothéties, $\circ$, $\langle$transformations euclidiennes, $\circ$, $\langle \mathcal{P}(A), \Delta \rangle$

Brève théorie

Propriété 1. Dans un groupe $\langle G, * \rangle$, $\exists$: élément neutre.

Propriété 2. Dans un groupe $\langle G, * \rangle$ $\forall a \in G$, $\exists$: $a' \in G$ tel que $a * a' = e = a' * a$.

Propriété 3. Dans un groupe $\langle A, * \rangle$ les lois de simplification sont valides, c'est-à-dire:
$a * b = a * c \Longrightarrow b = c$
$a * b = c * b \Longrightarrow a = c$.

Propriété 4. Dans un groupe $(a')' = a$.

Propriété .. Dans un groupe $(a * b)' = b' * a'$.

Définition: Si $\langle G, * \rangle$ est un groupe et si $B \subset G$ a toutes les propriétés de groupe lorsqu'on le munit de $*$, alors $\langle B, * \rangle$ est dit sous-groupe de G.

Propriété 6. Si $\langle G, * \rangle$ est un groupe et $\emptyset \neq B \subset A$, alors $\langle B, * \rangle$ est un sous-groupe $\Longleftrightarrow a, b \in B \Longrightarrow a * b' \in B$.

Démonstration:

$\Longrightarrow$ évident car B étant un sous groupe, $b \in B \Longrightarrow b' \in B$ et $a, b' \in B \Longrightarrow a * b' \in B$.

$\Longleftarrow$ Il faut montrer que $\langle B, * \rangle$ est un groupe.

Soit $c \in B$ alors $c * c' \in B$ et donc $e \in B$.

Soit $c \in B$ alors $e * c' \in B$ et donc $c' \in B$.

Soient $c, d \in B$ alors $c, d' \in B$ et donc $c * (d')' \in B$, c'est-à-dire $c * d \in B$.

L'associativité étant vraie dans G, elle l'est à fortiori dans B.

Propriété 7. Si $\langle G, * \rangle$ est un groupe fini, $\emptyset \neq B \subset A$ est un sous-groupe $\Longleftrightarrow a, b \in B \Longrightarrow a * b \in B$.

Propriété 8. Si $\emptyset \neq B \subset G$ où $\langle G, * \rangle$ est un groupe, l'ensemble de tous les "produits" finis d'éléments de B ou de symétriques d'éléments de B est un sous-groupe de G.

Démonstration:

Soient $a_1 * \ldots * a_n$ et $b_1 * \ldots * b_m$ deux tels "produits" où $a_i, b_i \in B$ ou $a_i', b_i' \in B$

alors $(a_1 *...* a_n) * (b_1 *...* b_m)' = (a_1 *...* a_n) * (b_m' *...* b_1')$ est encore un tel produit.
Par la propriété 6, il s'agit d'un sous-groupe.

Définition: On appelle le sous-groupe de la propriété 8 le sous-groupe engendré par B. Les éléments de B sont appelés générateurs. Lorsqu'on ne peut trouver d'ensemble de cardinalité plus petite pour engendrer ce sous-groupe, on dit que B est un ensemble minimal de générateurs. Si B peut se réduire à un seul élément, le sous-groupe engendré est dit cyclique.

Ainsi, dans les mouvements du carré $\{R_{90}, S_H\}$ est un ensemble de générateurs.

Dans $\langle \mathbb{Z}, + \rangle$, $\{1\}$ est un ensemble de générateurs. Ainsi $\mathbb{Z}$ est cyclique. Tous les $\langle \mathbb{Z}_n, + \rangle$ sont cycliques. $\langle \mathbb{Z}_5^*, x \rangle$ est cyclique.

Convention

Pour abréger les notations, il est d'usage, lorsqu'on traite des groupes abstraits non commutatifs, d'utiliser la notation multiplicative et la notation additive pour le cas commutatif.

Dictionnaire

$*$	x	$+$
e	1	0
a	a^{-1}	$-a$

On utilisera dans ce qui suit de la notation multiplicative.

Quelques résultats importants

Théorème de Lagrange

Si $\langle G, \bullet \rangle$ est un groupe fini d'ordre n et si $\langle B, \bullet \rangle$ est un sous-groupe d'ordre m, alors m divise n.

La preuve repose essentiellement sur la proposition qui suit.

Corollaire 1

Si $\langle G, \bullet \rangle$ est un groupe d'ordre premier, les seuls sous-groupes sont les sous-groupes triviaux: $\{1\}$ et G.

Corollaire 2

Si $\langle G, \bullet \rangle$ est un groupe d'ordre premier, il est cyclique et par conséquent commutatif.

Proposition 9. Si $\langle G, \bullet \rangle$ est un groupe et si B est un sous-groupe, les relations suivantes sur G sont des relations d'équivalence:

$$a \mathcal{R} b \Longleftrightarrow ab^{-1} \in B$$
$$a \mathcal{L} b \Longleftrightarrow a^{-1}b \in B$$

Définition: Lorsque $\mathcal{R} = \mathcal{L}$ on dit que B est un sous-groupe normal.

Définition: L'ensemble des "clubs" ou classes d'équivalence déterminées par $\mathcal{R}$ est appelé ensemble-quotient et noté $G/\mathcal{R}$. Idem pour $\mathcal{L}$.

Proposition 10. Si $\langle G, \bullet \rangle$ est un groupe et B un sous-groupe,

$$\mathcal{R} = \mathcal{L} \Longleftrightarrow axa^{-1} \in B \quad \forall x \in B \text{ et } \forall a \in G.$$

Preuve

Supposons que $\mathcal{R} = \mathcal{L}$, et soient $x \in B$ et $a \in G$. Alors $x^{-1} \in B$ et $a \in G$. Donc $x^{-1}a^{-1}a \in B$. D'où $x^{-1}a^{-1} \mathcal{R} a^{-1}$. D'où $x^{-1}a^{-1} \mathcal{L} a^{-1}$. D'où $axa^{-1} \in B$.

Supposons $axa^{-1} \in B \ \forall x \in B$ et $\forall a \in G$. Alors $a \mathcal{R} b \Longleftrightarrow ab^{-1} \in B$
$\Longleftrightarrow b^{-1} (ab^{-1}) (b^{-1})^{-1} \in B \Longleftrightarrow b^{-1} a \in B \Longleftrightarrow (b^{-1}a)^{-1} \in B$
$\Longleftrightarrow a^{-1}b \in B \Longleftrightarrow a \mathcal{L} b$.

Définition accessoire

Un sous-groupe B de G est dit normal $\Longleftrightarrow axa^{-1} \in B \ \forall x \in B$ et $\forall a \in G$.

Proposition 11

Si $\langle G, \bullet \rangle$ est un groupe commutatif, tout sous-groupe B est normal.

Démonstration:

Soient $x \in B$ et $a \in G$. Alors $xa^{-1}a \in B \Longrightarrow (xa^{-1})\ a \in B$
$\Longrightarrow a\ (xa^{-1}) \in B \Longrightarrow axa^{-1} \in B$.

(La réciproque est fausse)

Remarque:

Dans le cas où B est sous-groupe normal, l'ensemble-quotient $G/R = G/\mathcal{L}$ est noté plutôt G/B.

Proposition 12

Si $\langle G, \bullet \rangle$ est un groupe et B est un sous-groupe normal, l'ensemble-quotient G/B peut être muni d'une opération qui en fait un groupe, appelé groupe-quotient.

Démonstration:

Notons par Ca la classe d'équivalence de a déterminée par B. L'opération sera

$$Ca * Cb = C(a \bullet b)$$

a) Il faut vérifier que cette opération est bien définie, à savoir qu'elle ne dépend pas des représentants choisis.

Soient donc $a_1 \mathcal{R} a$ et $b_1 \mathcal{R} b$. Nous avons à vérifier que

$Ca_1 * Cb_1 = Ca * Cb$, ou

$C(a_1 \bullet b_1) = C(a \bullet b)$, ou

$a_1 b_1 \mathcal{R} ab$, ou

$a_1 b_1 b^{-1} a^{-1} \in B$.

Or, $a_1 \mathcal{R} a \Longrightarrow a_1 a^{-1} \in B$ et $b_1 \mathcal{R} b \Longrightarrow b_1 b^{-1} \in B$.

Mais $b_1 b^{-1} \in B \Longrightarrow a_1 (b_1 b^{-1}) a_1^{-1} \in B \Longrightarrow (a_1 b_1 b^{-1} a_1^{-1}) \overbrace{(a_1 a^{-1})}^{\in B} \in B$

$\Longrightarrow a_1 b_1 b^{-1} a^{-1} \in B$, ce qu'il fallait vérifier.

b) Vérifions qu'il s'agit d'une opération de groupe:

- $(Ca * Cb) * Cd = (C\ a\ b) * Cd = C(ab)\ d = C\ a\ (bd)$
  $= Ca * Cbd = Ca * (Cb * Cd)$ [associativité]

- $C1 * Cb = C1b = Cb = Cb1 = Cb * C1$

- Soit Ca alors Ca^{-1} est son symétrique car
  $Ca * Ca^{-1} = Caa^{-1} = C1 = Ca^{-1}a = Ca^{-1} * Ca$
  Ainsi $(Ca)^{-1} = Ca^{-1}$

Homomorphismes de groupes

Définition: $A \xrightarrow{f} B$ est dite injective si $f(a) = f(b) \Longrightarrow a = b$
(A et B sont des ensembles, f est une application)

$A \xrightarrow{f} B$ est dite surjective si $\forall\, y \in B$, $\exists\, x \in A$ tel que $f(x) = y$

$A \xrightarrow{f} B$ est dite bijective si elle est injective et surjective.

Définition: (produit fonctionnel)
Si $A \xrightarrow{f} B \xrightarrow{g} C$ sont des applications, on peut définir une application, notée gof, $A \xrightarrow{gof} C$ ainsi:

$$(gof)(x) = g(f(x)).$$

Proposition 13

Le produit fonctionnel est associatif.

Proposition 14

$A \xrightarrow{1_A} A$ où $1_A(x) = x$ $\forall x \in A$ est une bijection.

Définition: $A \xrightarrow{f} B$ est dite inversible si $\exists\, g: B \longrightarrow A$ telle que $gof = 1_A$ et $fog = 1_B$
g est alors notée f^{-1} et appelée inverse de f.

Remarque: la définition de f^{-1} est alors la suivante:

$$f^{-1}(x) = y \Longleftrightarrow f(y) = x.$$

Proposition 15
$A \xrightarrow{1_A} A$ est inversible.
De plus $1_A of = f$ et $gol_A = g$ $\forall f: B \longrightarrow A$ et $\forall g: A \longrightarrow C$.

Proposotion 16

a) Le produit de deux injections est une injection.
b) Le produit de deux surjections est une surjection.
c) Le produit de deux bijections est une bijection.

.Démonstration:

a) Soit $A \xrightarrow{f} B \xrightarrow{g} C$ où f et g sont des injections.
Soit (gof) (x) = (gof) (y), c'est-à-dire
g (f (x)) = g (f (y)). Or g est injective; alors
f (x) = f(y). Or f est injective; alors
x = y.

b) Soit $A \xrightarrow{f} B \xrightarrow{g} C$ où f et g sont des surjections.
Soit $z \in C$. g étant surjective, $\exists y \in B$ tel que g (y) = z.
f étant surjective, $\exists x \in A$ tel que f(x) = y.
Alors (gof) (x) = g (f (x)) = g (y) = z

c) conséquence de a) et b)

Proposition 17

a) Si gof est injective, alors f est injective.
b) Si gof est surjective, alors g est surjective.

Démonstration:

a) Supposons que f(x) = f(y).
Alors g (f (x)) = g (f (y)) c'est-à-dire (gof) (x) = (gof) (y).
Comme gof est injective, x = y.

b) Soit $A \longrightarrow B \xrightarrow{g} C$ et soit $z \in C$. Comme gof est surjective, $\exists x \in A$ tel que (gof) (x) = z c'est-à-dire g (f (x)) = z.

Proposition 18

$A \xrightarrow{f} B$ est bijective $\Longleftrightarrow$ elle est inversible.

Démonstration:

$\Longleftarrow$

$A \underset{g}{\overset{f}{\rightleftarrows}} B$ où $fog = 1_B \Longrightarrow$ g injective, f surjective

et $gof = 1_A \Longrightarrow$ f injective, g surjective

(Proposition 17 et Proposition 14.)

Ainsi f est bijective
et g est bijective.

$\Longrightarrow$

Supposons $A \xrightarrow{f} B$ bijective. Définissons $g: B \longrightarrow A$:

$g(y) = x$ tel que $f(x) = y$

g est bien définie car puisque f est bijective $\forall y, \exists! x$.

Et on vérifie que $gof = 1_A$ et $fog = 1_B$

(g est notée habituellement f^{-1})

Définition: Soit $\langle G_1, * \rangle \xrightarrow{f} \langle G_2, \# \rangle$

f est dit homomorphisme si $f(x * y) = f(x) \# f(y)$.
(Si G_1 et G_2 sont des groupes, on parle plutôt d'homomorphisme de groupe).

Exemples: $\langle \mathbb{R}, + \rangle \xrightarrow{\log} \langle \mathbb{R}^*, \times \rangle$

$\langle$Rotations du carré, $\circ \rangle \xrightarrow{f} \langle \mathbb{Z}_4, + \rangle$ où $f(R_0) = 0$, $f(R_{90}) = 1$, etc.

$\langle$translations du plan, $\circ \rangle \longrightarrow \langle \mathbb{C}, + \rangle$

$\langle \mathcal{P}(A), \cup \rangle \xrightarrow{f} \langle \mathcal{P}(A), \cap \rangle$ où f signifie "prendre le complément".

Proposition 19

Le produit (fonctionnel) de deux homomorphismes est un homomorphisme.

Démonstration:

Soient $\langle A, * \rangle \xrightarrow{f} \langle B, \# \rangle \xrightarrow{g} \langle C, \square \rangle$ des homomorphismes.
Alors $(gof)(x * y) = g(f(x * y)) = g(f(x) \# f(y))$
$= g(f(x)) \square g(f(y)) = (gof)(x) \square (gof)(y)$

Définition:

Si f est un homomorphisme injectif, il est dit monomorphisme.
Si f est un homomorphisme surjectif, il est dit épimorphisme.
Si f est un homomorphisme bijectif, il est dit isomorphisme.

Proposition 20

Le produit de 2 monomorphismes est un monomorphisme.
Le produit de 2 épimorphismes est un épimorphisme.
Le produit de 2 isomorphismes est un isomorphisme.

Démonstration: conséquences des propositions 16 et 19.

Proposition 21

$\langle A, * \rangle \xrightarrow{1_A} \langle A, * \rangle$ est un isomorphisme.

Proposition 22

Si gof est un monomorphisme, alors f est un monomorphisme.
Si gof est un épimorphisme, alors g est un épimorphisme.
(g et f sont des homomorphismes).

Démonstration: conséquences de la proposition 17.

Proposition 23

Si f est un isomorphisme, alors f^{-1} est un isomorphisme.

Démonstration:

Soit $\langle A, * \rangle \xrightarrow{f} \langle B, \# \rangle$ un isomorphisme.

Considérons $f^{-1}(x \# y)$. Or $f(x') = x \Longleftrightarrow f^{-1}(x) = x'$

et $f(y') = y \Longleftrightarrow f^{-1}(y) = y'$.

Alors $f^{-1}(x \# y) = f^{-1}(f(x') \# f(y')) = f^{-1}(f(x' * y'))$

$= x' * y' = f^{-1}(x) * f^{-1}(y)$.

Donc, f^{-1} est un homomorphisme. De plus, on sait qu'il est bijectif par la proposition 18.

Proposition 24

Soit $\langle G, \circ \rangle$ un groupe. L'ensemble des automorphismes de G (les isomorphismes de G dans G) forme un groupe si on le munit du produit fonctionnel.

Démonstration: conséquences de certaines des propositions précédentes.

De façon informelle, nous pouvons dire qu'un isomorphisme entre deux groupes assure leur "égalité" dans le sens que seule la symbolisation de leurs éléments et de leurs opérations diffère. Cette notion permet de reconnaître si deux situations en apparence distinctes sont algébriquement les mêmes. En effet le "nombre" d'éléments et la "table" d'opération sont les mêmes entre deux groupes isomorphes. Prenons comme exemples:

a) $\langle \mathbb{Z}, + \rangle$ et $\langle$nombres pairs, $+ \rangle$ avec $f(n) = 2n$

b) $\langle \{1, -1, i, -i\}, \times \rangle$ et $\langle \mathbb{Z}_4, + \rangle$
où $f(i) = 1$; $f(-1) = 2$; $f(-i) = 3$; $f(1) = 0$.

Cette notion est donc extrêmement importante en algèbre puisqu'elle apporte une grande économie de temps et de pensée en permettant de transposer tous les résultats algébriques découverts dans une situation à une autre situation mal connue mais isomorphe. C'est un outil universel en mathématiques puisque des notions adéquates d'isomorphismes sont utilisées dans presque toutes les branches des mathématiques.

Proposition 25

Si G_1 et G_2 sont deux groupes isomorphes, l'image d'un ensemble de générateurs de l'un est un ensemble de générateurs de l'autre et réciproquement.

(Preuve laissée en exercice).

Conséquence:

Pour savoir si deux groupes sont isomorphes, il suffit de comparer les ensembles minimaux de générateurs et de trouver une bijection de l'un sur l'autre qui engendre un isomorphisme. Un élément d'ordre n est envoyé sur un élément du même ordre.

Proposition 26

Si $\langle A, \cdot \rangle \xrightarrow{f} \langle B, \cdot \rangle$ est un homomorphisme de groupe,

a) $f(1)$ est le neutre de B

b) $f(a)^{-1} = f(a^{-1})$

c) $\langle f(a), \cdot \rangle$ est un sous-groupe de $\langle B, \cdot \rangle$.

Démonstration laissée en exercice.

Proposition 27

Soit $A \xrightarrow{f} B$ un homomorphisme de groupe. Alors
$\text{noy}f = \{x \in A \mid f(x) = 1\}$ est un sous-groupe normal dans A.

Démonstration laissée en exercice.

Définition:

Si $A \xrightarrow{f} B$ est un homomorphisme de groupe, l'application $noyf \xrightarrow{i} A$ où $i(x) = x$ est appelé injection canonique, et $A \xrightarrow{\P} A/_{noyf}$ où $\P(x) = Cx$ est appelé projection canonique.

Proposition 28

Si $A \xrightarrow{f} B$ est un homomorphisme de groupe, considérons la suite:

$$noyf \xrightarrow{i} A \xrightarrow{\P} A/_{noyf}.$$

Alors i est un monomorphisme,
¶ est un épimorphisme,
$\P i = o$ (où $o(x) = \forall x$),
$noy\P = imi$ $(imi = \{y \in A \mid \exists x \in noyf \text{ et } i(x) = y\} = i(a))$.

Exercices sur les groupes

1. Dans le groupe des mouvements du carré, trouver les sous-groupes normaux. Construire les ensembles-quotients correspondants. Seront-ils des groupes?

2. Existe-t-il un isomorphisme entre le groupe des quaternions (8 éléments) et le groupe des trois commutateurs? Sinon, pourquoi?

Proposition 29

Soit $G_1 \xrightarrow{f} G_2 \underset{h}{\overset{g}{\rightrightarrows}} G_3$ des homomorphismes de groupes.

Si f est un épimorphisme alors gof = hof $\Longrightarrow$ g = h.

Démonstration:

Supposons f un épimorphisme et supposons que gof = hof. Soit $y \in G_2$. Alors $\exists x \in G_1$ tel que f(x) = y puisque f est surjectif.

Ainsi g(y) = g(f(x)) = h(f(x)) = h(y). Donc g = h.

Proposition 30

Soit $G_1 \underset{h}{\overset{g}{\rightrightarrows}} G_2 \xrightarrow{f} G_3$.

Si f est un monomorphisme, alors fog = foh $\Longrightarrow$ g = h.

Démonstration:

Supposons fog = foh alors $\forall x \in G_1$,

$$f(g(x)) = f(h(x)).$$

Comme f est un monomorphisme, $g(x) = h(x)\ \forall x \in G_1$.

Ainsi g = h.

Remarque: Les réciproques des propositions 29 et 30 sont vraies, mais ne sont faciles à démontrer.

2. Les anneaux

L'exemple fondamental d'anneau est $\mathbb{Z}$ muni de + et x. L'étude théorique des anneaux permet de déduire en particulier sous forme de théorèmes les propriétés algébriques de $\mathbb{Z}$, par exemple la théorie des exposants entiers, quelques lois classiques de l'algèbre, etc.. C'est aussi à l'aide des résultats généraux sur les anneaux et de relations d'équivalence appropriées que l'on peut construire $\mathbb{Z}$ à partir de $\mathbb{N}$. Plusieurs résultats et notions de la théorie des groupes ont leurs analogues pour les anneaux. C'est d'ailleurs l'analogie entre les résultats et ceux d'autres structures qui a conduit à l'élaboration du langage des catégories.

Définition:

Un anneau est un ensemble A muni de deux opérations, notées symboliquement + et x, et répondant aux axiomes suivants:

A_1) $\langle A, + \rangle$ est un groupe commutatif,

A_2) x est fermée,

A_3) x est associative,

A_4) il existe un neutre pour x, noté symboliquement 1.

A_5) $\forall a, b, c \in A$, $a(b + c) = ab + ac$ [distributivité à gauche]
$(a + b)c = ac + bc$ [distributivité à droite]

on note l'anneau $\langle A, +, \times \rangle$

Remarque: Si de plus x est commutative, on dit que l'anneau est commutatif.

Exemples d'anneaux:

$\langle \mathbb{Z}, +, \times \rangle$, $\langle \mathcal{P}(A), \Delta, \cap \rangle$ $\langle \mathbb{Z}_n, +, \times \rangle$ $\langle \mathbb{Q}, +, \times \rangle$

$\langle$Polynomes sur $\mathbb{Z}$, +, x$\rangle$, $\langle$fonctions de $\mathbb{R}$ dans $\mathbb{R}$, +, $\circ\rangle$, etc.

Exercice: Est-ce que $\langle \mathbb{Q}, +, * \rangle$ où $a * b = a + b + ab$

$\langle \mathbb{Q}, \#, x \rangle$ où $a \# b = \sqrt[3]{a^3 + b^3}$

sont des anneaux?

"Dictionnaire" entre groupe et anneau

groupe	anneau
sous-groupe	sous-anneau
sous-groupe engendré	sous-anneau engendré
sous-groupe normal	idéal
homomorphisme de groupe	homomorphisme d'anneau
noy f = sous-groupe normal	noy f = idéal
groupe-quotient $G/_B$	anneau- quotient $A/_I$
etc.	etc..

Définition:

$A \xrightarrow{f} B$, A, B anneaux, est dit homomorphisme d'anneau
si $f(x + y) = f(x) + f(y)$
et $f(xy) = f(x)\, f(y)$.

Exemple d'homomorphisme d'anneau:
$\langle \mathbb{Z}, +, x \rangle \xrightarrow{f} \langle \mathbb{Z}_n, +, \cdot \rangle$ où $f(x) = Cx$.

3. Corps

L'exemple de corps est $\mathbb{Q}$ muni de + et x. La théorie générale des corps permet de déduire en particulier, sous forme de théorèmes, les propriétés algébriques des rationnels, par exemple la théorie des proportions, la théorie des radicaux, etc.. C'est à l'aide des résultats sur les anneaux et en utilisant des relations d'équivalence appropriées que l'on peut construire $\mathbb{Q}$ à partir de $\mathbb{Z}$.

Définition:

Un corps est un ensemble $\mathbb{K}$, muni de deux opérations, notées symboliquement + et x, et répondant aux conditions suivantes:

C_1) $\langle \mathbb{K}, +, x \rangle$ est un anneau commutatif.

C_2) $\forall\, o \neq a \in C, \exists a^{-1}$ tel que $a\, a^{-1} = 1$

Remarque: on parle de corps gauche si la x n'est pas commutative.

Exemples de corps:

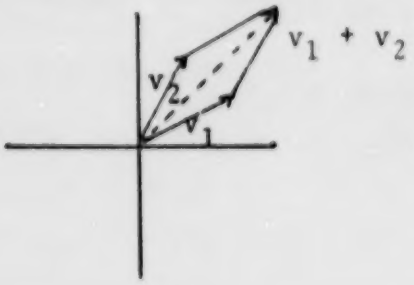
$\langle \mathbb{Q}, +, x \rangle$, $\langle \mathbb{R}, +, x \rangle$, $\langle \mathbb{Q}, +, x \rangle$, $\langle \mathbb{Z}_p, +, x \rangle$

$\langle$Quaternions, +, x$\rangle$, $\langle \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}, +, x \rangle$ etc..

4. Espaces vectoriels sur un corps

L'exemple typique des espaces vectoriels est l'ensemble des vecteurs du plan.

Soit V l'ensemble des vecteurs du plan liés à une origine o.



Si + est définie comme suit: $v_1 + v_2$ = vecteur formé par la diagonale du parallélogramme construit sur v_1 et v_2.

On peut alors vérifier que $\langle V, + \rangle$ est un groupe commutatif.

Si de plus $x \bullet v$, où $x \in R$, désigne le vecteur obtenu de v en multipliant sa longueur par x, on constate que:

$$1) \quad 1 \bullet v = v$$
$$2) \quad (xy) \bullet v = x \bullet (y \bullet v)$$
$$3) \quad (x + y) \bullet v = x \bullet v + y \bullet v$$
$$4) \quad x \bullet (u + v) = x \bullet u + x \bullet v.$$

Cette deuxième opération du type $R \times V \longrightarrow V$ est

$$(x, v) \longrightarrow x \bullet v$$

appelée multiplication scalaire.

Définition:

Un espace vectoriel sur un corps K est un ensemble V muni de deux opérations, notées symboliquement + et •, du type:

$$V \times V \longrightarrow V \qquad \text{et} \qquad K \times V \longrightarrow V$$
$$(v_1, v_2) \rightsquigarrow v_1 + v_2 \qquad (x, v) \rightsquigarrow x \bullet v$$

et satisfaisant aux conditions suivantes:

V_1) $\langle V, + \rangle$ est un groupe commutatif

V_2) $1 \bullet v = v$

V_3) $(xy) \bullet v = x \bullet (y \bullet v)$

V_4) $(x + y) \bullet v = x \bullet v + y \bullet v$

V_5) $x \bullet (u + v) = x \bullet u + x \bullet v.$

Exemples d'espace vectoriel:

$\langle$vecteurs de l'espace, +, •$\rangle$ sur $\mathbb{Q}$ ou $\mathbb{R}$; $\langle$Vecteurs sur la droite, +, •$\rangle$ sur $\mathbb{R}$,

<Polynômes sur $\mathbb{Q}$, +, •> sur $\mathbb{Q}$;

<$\mathbb{Q}$, +, x> sur $\mathbb{Q}$;

<le plan euclidien, +, •> sur $\mathbb{R}$ où $(a, b) + (c, d) = (a + c, b + d)$

$x \bullet (a, b) = (xa, xb)$

Remarque:

Le dernier exemple n'est qu'une reformulation de l'exemple donné avec les vecteurs du plan.

Définition:

Si V_1 et V_2 sont des espaces vectoriels sur K, $V_1 \xrightarrow{f} V_2$ est dit homomorphisme d'espace vectoriel ou, plus précisément, transformation linéaire si

$$f(v_1 + v_2) = f(v_1) + f(v_2)$$

$$\text{et } f(x \bullet v_2) = x \bullet f(v_1)$$

Ainsi, on peut vérifier que les rotations, les symétries et les homothéties sont des transformations linéaires (et même des isomorphismes, c'est-à-dire des transformations linéaires bijectives) du plan euclidien en lui-même.

Pour mieux étudier les transformations linéaires (et par conséquent certaines transformations géométriques), les mathématiciens ont trouvé le moyen de les représenter par des matrices de nombres sur lesquelles ils ont mis des opérations correspondant aux opérations somme et produit fonctionnel et de développer ainsi un calcul "mécanique" plus malléable. L'explication de ce procédé est en dehors des objectifs de ce cours.

Si, depuis quelques générations, la géométrie occupe une place de moins en moins importante dans le curriculum des collèges de certains pays, c'est en grande partie dû au fait que

le développement de la théorie des espaces vectoriels a permis de la traiter de façon algébrique ou "arithmétique". Choquet et Dieudonné, en France, peuvent être tenus pour être parmi les grands responsables de ce changement.

Exercices

1. Soit $V = \{(a, b) \mid a, b \in \mathbb{R}\}$ le plan euclidien muni des opérations

   a) $V \times V \longrightarrow V$ où $(a, b) + (c, d) = (a + c, b + d)$

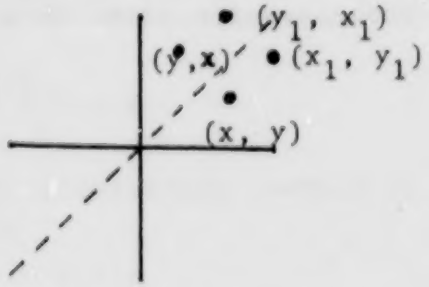
   b) $\mathbb{R} \times V \longrightarrow V$ où $x\,(a, b) = (xa, xb)$

   qui en font un espace vectoriel sur $\mathbb{R}$.

   Considérons $V \xrightarrow{f} V$ où $f(x, y) = (y, x)$.
   Vérifier que f est un isomorphisme d'espace vectoriel.

   Remarque: f est une symétrie par rapport à la diagonale principale du plan.

   La matrice associée à f pourrait être $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$



2. Vérifier que $\langle \mathbb{Q}, +, \times \rangle$ est un espace vectoriel sur $\mathbb{Q}$.

3. Vérifier que le plan euclidien tel que défini en 1. est isomorphe à l'ensemble des vecteurs du plan, muni de la somme et de la multiplication scalaire telles que définies plus haut.

Annexe au chapitre I

Exercice MAT 4883

Voici le "système d'axiomes" de Piaget sur les "groupements":

G_1 Deux éléments quelconques d'un groupement peuvent être composés entre eux et ils engendrent un nouvel élément de même groupement:

$$x + x' = y,\ y + y' = z.$$

G_2 Toute transformation est "réversible":

$$y - x = x' \quad \text{ou} \quad y - x' = x.$$

G_3 La composition des opérations est associative:

$$(x + x') + y' = x + (x' + y') = z.$$

G_4 Une opération combinée avec son inverse est annulée:

$$x - x = 0 \qquad y - y = 0.$$

G_5 Un élément quantitatif répété ne se transforme pas:

$$x + x = x \qquad y + y = y.$$

Problème:

Montrer qu'un ensemble satisfaisant à ces axiomes ne peut être que trivial.

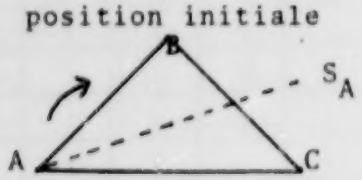
Attention: il faut prendre G_2 tel qu'énoncé.

Tables de groupes

Triangle:

	R_0	R_{120}	R_{240}	S_A	S_B	S_C
R_0	R_0	R_{120}	R_{240}	S_A	S_B	S_C
R_{120}	R_{120}	R_{240}	R_0	S_B	S_C	S_A
R_{240}	R_{240}	R_0	R_{120}	S_C	S_A	S_B
S_A	S_A	S_C	S_B	R_0	R_{240}	R_{120}
S_B	S_B	S_A	S_C	R_{120}	R_0	R_{240}
S_C	S_C	S_B	S_A	R_{240}	R_{120}	R_0

position initiale



S_3:

	I	(12) (13)	(13) (12)	(12)	(23)	(13)
I	I	(12) (13)	(13) (12)	(12)	(23)	(13)
(12) (13)	(12) (13)	(13) (12)	I	(23)	(13)	(12)
(13) (12)	(13) (12)	I	(12) (13)	(13)	(12)	(23)
(12)	(12)	(13)	(23)	I	(13) (12)	(12) (13)
(23)	(23)	(12)	(13)	(12) (13)	I	(13) (12)
(13)	(13)	(23)	(12)	(13) (12)	(12) (13)	I

position initiale: 1 2 3.

3 commutateurs

	000	001	010	011	100	110	101	111
000	000	001	010	011	100	110	101	111
001	001	000	011	010	101	111	100	110
010	010	011	000	011	110	100	111	101
011	011	010	001	000	111	101	110	100
100	100	101	110	111	000	010	001	011
110	110	111	100	101	010	000	011	101
101	101	100	111	110	001	011	000	010
111	111	110	101	100	011	101	010	000

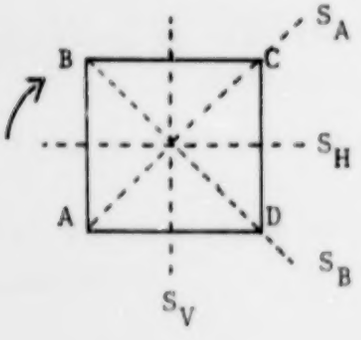
Quaternions

X	1	-1	i	-i	j	-j	k	-k
1	1	-1	i	-i	j	-j	k	-k
-1	-1	1	-i	i	-j	j	-k	k
i	i	-i	-1	1	k	-k	-j	j
-i	-i	i	1	-1	-k	k	j	-j
j	j	-j	-k	k	-1	1	i	-i
-j	-j	j	k	-k	1	-1	-i	i
k	k	-k	j	-j	-i	i	-1	1
-k	-k	k	-j	j	i	-i	1	-1

Mouvements du carré

	R_0	R_{90}	R_{180}	R_{270}	S_A	S_B	S_H	S_V
R_0	R_0	R_{90}	R_{180}	R_{270}	S_A	S_B	S_H	S_V
R_{90}	R_{90}	R_{180}	R_{270}	R_0	S_V	S_H	S_A	S_B
R_{180}	R_{180}	R_{270}	R_0	R_{90}	S_B	S_A	S_V	S_H
R_{270}	R_{270}	R_0	R_{90}	R_{180}	S_H	S_V	S_B	S_A
S_A	S_A	S_H	S_B	S_V	R_0	R_{180}	R_{90}	R_{270}
S_B	S_B	S_V	S_A	S_H	R_{180}	R_0	R_{270}	R_{90}
S_H	S_H	S_B	S_V	S_A	R_{270}	R_{90}	R_0	R_{180}
S_V	S_V	S_A	S_H	S_B	R_{90}	R_{270}	R_{180}	R_0

position initiale



Exercices sur les groupes (MAT 4883)

Vérifier si les systèmes suivants constituent des groupes:

<Polynômes à coefficients dans $\mathbb{R}$, +>

<$\mathbb{Q} \setminus \{0\}$, x>

<$\mathcal{P}(A)$, Δ>

<$\mathbb{Z}_4 \setminus \{0\}$, x>, <$\mathbb{Z}_7 \setminus \{0\}$, x>, <$\mathbb{Z}_2$, +>

<{1, -1, i, -i}, x> où $i = \sqrt{-1}$

<Mouvements du triangle, *>

<$\{f_1, f_2, f_3, f_4, f_5, f_6, \}^{\circ}$> où $f_1(x) = x$, $f_2(x) = 1/_{1-x}$, $f_3(x) = \frac{x-1}{x}$

$f_4(x) = 1/_x$, $f_5(x) = 1-x$,

$f_6(x) = x/_{x-1}$

et $f_i: \mathbb{R} \longrightarrow \mathbb{R}$.

<$\mathbb{Q}$, *> où $a * b = a + b + ab$

<$\mathbb{R}$, *> où $a * b = \sqrt[3]{a^3 + b^3}$

<S_3, *> où S_3 est l'ensemble des permutations de trois objets.

-Démontrer que si B et C sont des sous-groupes de <A, *> alors $B \cap C$ est un sous-groupe de <A, *>.

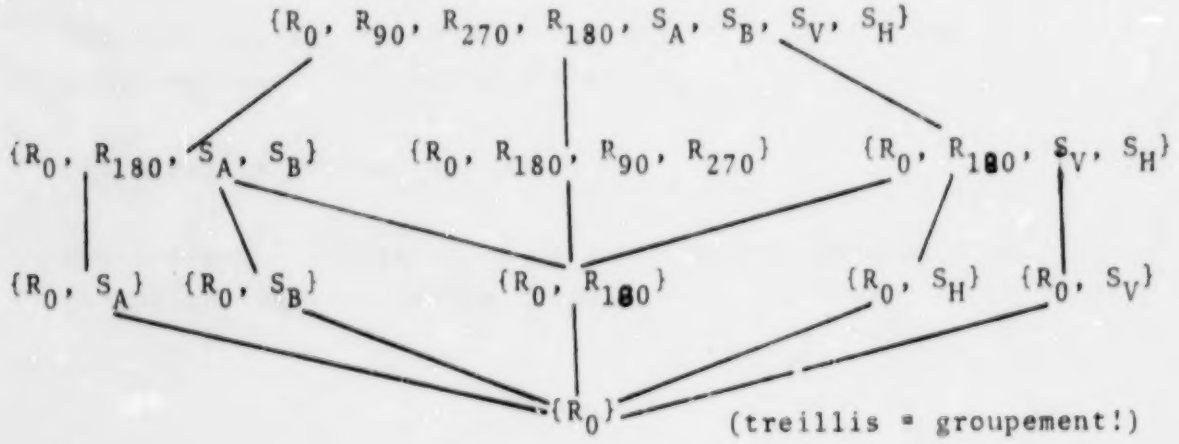
-Démontrer que le symétrique est unique dans un groupe.

-Démontrer que le symétrique du symétrique d'un élément d'un groupe est cet élément.

Treillis des sous-groupes du groupe des mouvements du carré.

Méthode de recherche:

Les sous-groupes seront d'ordre 1, 2, 4 ou 8. (Lagrange).
Ceux d'ordre 1 et 8 sont les sous-groupes triviaux: $\{R_0\}$ et groupe entier.
Ils doivent tous contenir R_0.
Il suffit de chercher les sous-ensembles fermés (prop. 7).
Chaque élément qui est son propre symétrique forme un sous-groupe avec R_0.



(treillis = groupement!)

Les sous-groupes d'ordre 4 sont forcément normaux car pour R et S une des classes est constituée du sous-groupe ne laissant pas de choix pour l'autre classe.

$\{R_0\}$ induit une partition en 8 classes pour R et S. Il est donc normal.

Ce groupe entier induit une partition en une seule classe pour R et S. Il est donc normal.

$\{R_0, S_A\}$: $S_H S_A S_H^{-1} = S_H S_A S_H = S_B \notin \{R_0, S_A\}$. Donc pas normal.

$\{R_0, S_B\}$: $S_H S_B S_H^{-1} = S_H S_B S_H = S_A \notin \{R_0, S_B\}$. Donc pas normal.

$\{R_0, S_H\}$: $S_A S_H S_A^{-1} = S_A S_H S_A = S_V \notin \{R_0, S_H\}$. Donc pas normal.

$\{R_0, S_V\}$: $S_A S_V S_A^{-1} = S_A S_V S_A = S_H \notin \{R_0, S_V\}$. Donc pas normal.

$\{R_0, R_{180}\}$: $R = \underline{|R_0\ R_{180}|\ |R_{90}\ R_{270}|\ |S_A\ S_B|\ |S_V\ S_H|}$

$S = \underline{|R_0\ R_{180}|\ |R_{90}\ R_{270}|\ |S_A\ S_B|\ |S_V\ S_H|}$

$R = S$. Donc normal.

Exercices sur le chapitre I

. Définir un isomorphisme entre le groupe des mouvements du triangle et le groupe S_3 des permutations de 3 objets.

.. Vérifier que $f(n) = 2n$ est un isomorphisme entre
$\langle \mathbb{Z}, + \rangle$ et $\langle$Pairs, $+\rangle$
trouver noy f et $\mathbb{Z}/_{\text{noy } f}$

. Même question que la précédente en remplaçant $\langle$Pairs, $+\rangle$ par $\langle \mathbb{Z}, + \rangle$.

. Vérifier que $\langle \mathbb{Z}, + \rangle \xrightarrow{f} \langle \mathbb{Z}, + \rangle$ où $f(n) = o \ \forall n \in \mathbb{Z}$ est un homomorphisme. Trouver noy f et $\mathbb{Z}/_{\text{noy } f}$.

. Démontrer la proposition 26.

. Montrer que l'intersection de sous-groupes normaux d'un groupe est un sous-groupe normal.

CHAPITRE II

Catégories et groupements

§1 Historique du langage des catégories

Nous avons tenté dans le chapitre précédent de faire ressortir, particulièrement en théorie des groupes, certaines notions ou résultats qui, formellement, se retrouvent dans l'étude de plusieurs structures. Ainsi en est-il des notions de sous-structure (sous-groupe, sous-anneau, etc.), d'homomorphisme, de structure-quotient, de noy et de Image, des propositions 17, 19, 20, 28, 29, 30 pour n'en citer que quelques-unes. Les mathématiciens qui ont approfondi ces diverses structures algébriques ou autres avant 1945 constataient et découvraient des ressemblances de plus en plus nombreuses. Le rôle des fonctions préservant les structures (homomorphismes) apparaissait comme fondamental, mais les propriétés auxquelles elles semblaient répondre n'étaient cependant pas explicitées. Les transferts des méthodes de recherche, des résultats et des outils d'une structure à un autre étaient chose courante chez les mathématiciens.

Ce sont les mathématiciens CARTAN et EILENBERG qui les premiers expliciteront les ressemblances en développant dans un article paru en 1945 un nouveau langage des catégories. Ils mirent en évidence une structure des "homomorphismes" communes à un très grand nombre de structures (algébriques ou non). Par la suite, dans un volume célèbre, datant de 1956, intitulé "Homological Algebra", ils traîtèrent de sphères avancées de l'algèbre à l'aide de ces nouveaux outils. Plus tard, ce langage permettra de transférer certains outils et méthodes algébriques à d'autres domaines, particulièrement en topologie et en géométrie.

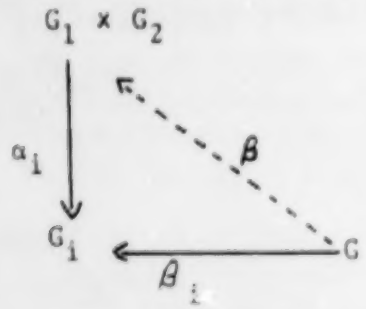
Les notions et résultats qui pourront facilement se transférer d'une structure à une autre et qui, par conséquent, intéresseront le langage des catégories, seront ceux pouvant se formuler sans faire appel aux éléments particuliers de ces structures. Des exemples typiques de tels résultats se trouvent aux propositions 28, 29 et 30. Les propositions 29 et 30 serviront même à définir les notions de monomorphisme et d'épimorphisme dans une structure quelconque. Plusieurs notions ont été reformulées dans ce but. Voici un exemple de ce fait.

Si $\langle G_1, * \rangle$ et $\langle G_2, \# \rangle$ sont deux groupes, on peut définir un nouveau groupe, appelé produit direct de G_1 et G_2 comme suit:

$\langle G_1 \times G_2, \bullet \rangle$

ou $(a, b) \bullet (c, d) = (a * c, b \# d)$

or, il a la propriété caractéristique suivante:



où $\alpha_i\ (a_1, a_2) = a_i$

β_i homomorphisme

G quelconque

β homomorphisme.

$\forall G$ et $\forall \{\beta_i\}_{i = 1,2}$, $\exists!\ \beta$ tel que $\alpha_i \beta = \beta_i$.

Pour des fins de langage des catégories, on a donc défini $G_1 \times G_2$ comme étant le seul groupe muni des $\{\alpha_i\}_{i = 1,2}$ ayant cette propriété. Cette définition peut alors s'étendre à d'autres structures.

§2. Langage des catégories

1. Définition de catégorie et exemples

Une catégorie $\mathcal{C}$ est un triplet (S, T, o) où:

-S est un "ensemble" dont les éléments A, B, C, ... sont appelés objets de la catégorie.

-T est un ensemble dont les éléments f, g, h, ... sont appelés morphismes de la catégorie: pour tout couple d'objets (A, B), il existe un ensemble (possiblement vide) $M(A, B) \subseteq T$
$f \in M(A, B)$ s'écrit habituellement $f: A \longrightarrow B$.

-o est une opération partielle sur T du type:
$M(A, B) \times M(B, C) \longrightarrow M(A, C)$
$(f, g) \longrightarrow g \circ f$
et satisfaisant aux axiomes suivants:

C_1: un morphisme attaché à un couple ne peut être confondu avec un morphisme attaché à un autre couple.
$(M(A, B) \cap M(C, D) = \emptyset$ si $A \neq C$ ou $B \neq D)$

C_2: l'opération partielle o est associative, c'est-à-dire:
$f \circ (g \circ h) = (f \circ g) \circ h$.

C_3: chaque objet A possède un morphisme unité, noté 1_A, c'est-à-dire:
$1_A \circ f = f$ et $g \circ 1_A = g \quad \forall f$ et $\forall g$.

Remarques

a) on démontre facilement que 1_A est unique $\forall A$

b) le symbolisme généralement utilisé est le suivant:
$\mathcal{C}$: catégorie
$\mathcal{O}$: objets
$\mathcal{M}$: morphismes.

Nous avons changé le symbolisme habituel pour l'adapter à celui qu'utilise Wittmann pour définir les groupements.

Exemples de catégories

Les catégories ayant été développées pour décrire la "structure" des structures algébriques classiques, c'est dans ce domaine que nous retrouvons les principaux exemples.

-Les ensembles (S) avec les applications (T) et le produit fonctionnel (o) constituent une catégorie, habituellement notée Ens..

Explications:

. M (A, B) = ensemble des applications de A à B.

. Si f: $A \longrightarrow B$ et g: $B \longrightarrow C$ sont des applications, gof: $A \longrightarrow C$ est encore une application.

. ho (gof) = (hog) of si $A \xrightarrow{f} B \xrightarrow{g} C \xrightarrow{h} D$. (C_2) (Prop. 13)

. 1_A: $A \longrightarrow A$ est bien un morphisme unité (C_3) (Prop. 15)

C_1 est assuré par la définition d'application.

-Les ensembles (S) avec les applications injectives (T) (respectivement surjectives ou bijectives) et le produit fonctionnel (o) constituent une catégorie.

Assuré par les propositions 14, 16, 15.

-Les groupes (S) avec les homomorphismes de groupe (T) et le produit fonctionnel (o) constituent une catégorie.

Assuré par les propositions 19, 21, 15.

-Les groupes (S) avec les monomorphismes (T) (respectivement les épimorphismes ou isomorphismes) et le produit fonctionnel (o) constituent une catégorie habituellement notée G.

Assuré par les propositions 20, 21, 15.

-Les monoïdes (S) avec les homomorphismes (T) et le produit fonctionnel (o) constituent une catégorie.

-Les ensembles ordonnés (S) avec les fonctions monotones (morphismes pour l'ordre) (T) et le produit fonctionnel (o) constituent une catégorie habituellement notée Ord..

cf. cours MAT 4823, notes de D. Lunkenbein, p. 13 et sq.

f: $\langle A, \leq \rangle \longrightarrow \langle A', \leq' \rangle$ est monotone si $a \leq b \Longrightarrow f(a) \leq' f(b)$.

Exercice: montrer que le produit de deux fonctions monotones est une fonction monotone, et que 1_A est monotone.

-Le treillis (S) avec les morphismes de treillis (T) et le produit fonctionnel (o) constituent une catégorie.

f: $(T, \sqcap, \sqcup) \longrightarrow (T_1, \sqcap', \sqcup')$ est dit homomorphisme de treillis si

$$f(a \sqcup b) = f(a) \sqcup' f(b)$$
$$f(a \sqcap b) = f(a) \sqcap' f(b).$$

Exercice: vérifier que le produit fonctionnel de deux homomorphisme de treillis est encore un homomorphisme de treillis et que 1_A est un homomorphisme de treillis.

-Les graphes (S) avec les homomorphismes de graphes (T) et le produit fonctionnel (o) constituant une catégorie notée Grph..

ρ: $(X, U) \longrightarrow (X', U')$ est dit morphisme de graphe si ρ est une double fonction de X dans X' et de U dans U' qui "respecte" les rapports entre arcs et sommets. (Pour une définition plus précise, cf. Maclane, Categories for the working mathematician, p.48).

-De façon générale, la classe des ensembles munis d'une même structure (S) avec les applications conservant cette structure (T) et le produit fonctionnel (o) constituent une catégorie.

-Les ensembles (S) avec les relations (T) et le produit relationnel (o) constituent une catégorie notée Rel..

M (A, B) désigne toutes les relations de A vers B.

Si $A \xrightarrow{S} B \xrightarrow{R} C$ sont des relations.

$RoS = \{(x, z) \mid \exists y \in B \text{ et } (x, y) \in S \text{ et } (y, z) \in C\}$.

-Les catégories (S) avec les fonctions (T) et le produit fonctoriel (o) constituent une catégorie notée Cat..

-La catégorie des anneaux, la catégorie des corps, la catégorie des espaces vectoriels sur K.

Les structures précédentes constituent le type d'exemples que visait originellement le langage des catégories, c'est-à-dire des classes d'ensembles munis d'une même structure. On a cependant rapidement réalisé que la notion de catégorie pouvait aussi servir à décrire la structure interne d'un seul ensemble. C'est dans cette optique que Wittmann utilise la notion de catégorie pour définir les groupements.

Voici donc quelques exemples où les objets sont constitués par les éléments d'un ensemble.

Un ensemble quelconque A sans structure peut être considéré comme une catégorie, appelée catégorie discrète, si l'on ajoute arbitrairement une flèche identité à chaque élément:

$$(A, \{1_x\}_{x \in A}, \circ)$$

. Le graphe orienté d'un ensemble préordonné P (réflexif et transitif) est une catégorie.

Objets: éléments de P
morphismes: flèches du graphe
$(a \longrightarrow b) \circ (b \longrightarrow c) = a \longrightarrow c$ (assuré par la transitivité)
les morphismes unités sont assurés par la réflexivité.

En particulier, un ensemble ordonné, un ensemble muni d'une relation d'équivalence, un treillis peuvent être considérés comme des catégories.

Il suffit de définir l'ordre naturel sur le treillis:

$$a \mathcal{R} b \Longleftrightarrow a \sqcap b = a.$$

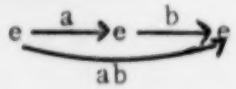
Et ainsi, dans les trois cas, les morphismes sont $\{a \mathcal{R} b \mid a, b \in A\}$ et la loi de composition $(a \mathcal{R} b) \circ (b \mathcal{R} c) = a \mathcal{R} b$ est assurée par la transitivité des relations. L'existence d'unités est assurée par la réflexivité des relations.

Cette loi de composition pourra se réécrire:

$$(a, b) \circ (b, c) = (a, c)$$

si on sous-entend $(a, b), (b, c), (a, c) \in \mathcal{R}$.

Un monoïde est une catégorie à un seul objet (l'élément neutre), dont les morphismes sont les éléments du monoïde et dont la loi de composition est l'opération du monoïde:



En particulier, un groupe est une catégorie à un seul objet.

Ainsi, $\mathbb{Z}$ et $\mathbb{N}$ peuvent être considérés comme des catégories à plusieurs points de vue ... .

Quelques notions et définitions sur les catégories

Morphisme inversible:

Dans une catégorie $\mathcal{C}$, $f: A \longrightarrow B$ est dit inversible s'il existe $g: B \longrightarrow A$ tel que $gof = 1_A$ et $fog = 1_B$. g est alors appelé inverse de f et est noté f^{-1}. f est aussi appelé un isomorphisme.

Ainsi, dans le graphe d'un ensemble pré-ordonné, les morphisme inversibles (ou isomorphismes) sont les constituants des paires boomerang. Dans un groupe tout morphisme est inversible. Quels seraient les morphismes inversibles dans la catégorie des ensembles et des applications? Dans celle des groupes? Dans celle des ensembles ordonnés? Dans celle des treillis?

Groupoïde

Une catégorie où tout morphisme est inversible est appelée GROUPOIDE. Y a-t-il des groupoïdes parmi les exemples de catégories citées plus haut?

Monomorphisme et épimorphisme

Dans une catégorie $\mathcal{C}$, $f: A \longrightarrow B$ est dit monomorphisme (respectivement épimorphisme) si $fog = foh \Longrightarrow g = h$ (simplification à gauche) [respectivement si $gof = hof \Longrightarrow g = h$ (simplification à droite)].

On peut montrer assez facilement que tout isomorphisme d'une catégorie est un monomorphisme et un épimorphisme, mais la réciproque est fausse.

Dans la plupart des catégories importantes, où les morphismes sont en particulier des applications, on peut montrer (plus ou moins facilement) que

monomorphismes $\Longleftrightarrow$ injections
épimorphismes $\Longleftrightarrow$ surjections
isomorphismes $\Longleftrightarrow$ isomorphismes de structure.

Sous-catégorie

Soit $\mathcal{C}$ une catégorie; $\mathcal{C}'$ sera dite sous-catégorie de $\mathcal{C}$ si

a) les objets de $\mathcal{C}'$ sont des objets de $\mathcal{C}$
b) les morphismes de $\mathcal{C}'$ sont des morphismes de $\mathcal{C}$
c) l'opération partielle dans $\mathcal{C}'$ est induite par celle de $\mathcal{C}$
d) $\mathcal{C}'$ est une catégorie.

Exemples de sous-catégories:

La catégorie des ensembles finis est sous-catégorie de la catégorie des ensembles.

La catégorie des groupes abéliens est sous-catégorie des groupes.

({1, 2, ..., 10}, relation divise) est sous-catégorie de (Z, relation divise)

(hexagones convexes, plus "parfait" ou égal) est sous-catégorie de (hexagones, plus "parfait" ou égal)

etc..

Sous-catégorie pleine

Une sous-catégorie $\mathcal{C}'$ est dite pleine dans $\mathcal{C}$ si

$$M_{\mathcal{C}'}(A, B) = M_{\mathcal{C}}(A, B).$$

Les exemples précédents sont des sous-catégories pleines.

La catégorie des anneaux n'est pas pleine dans la catégorie des groupes. $(\mathbb{Z}, \cdot)$ n'est pas pleine dans $(\mathbb{Z}, \leq)$.

Produit direct de catégories

Si $\mathcal{C}_1$ et $\mathcal{C}_2$ sont deux catégories, on peut définir une nouvelle catégorie, appelée catégorie produit et notée $\mathcal{C}_1 \times \mathcal{C}_2$ comme suit:

les objets sont $\{(A, A_2) \mid A_i \in \mathcal{C}_i\}$

$$(A_1, A_2) \xrightarrow[(f_1, f_2)]{} (B_1, B_2) \text{ si } f_i : A_i \longrightarrow B_i$$

$$(A_1, A_2) \xrightarrow{(f_1, f_2)} (B_1, B_2) \xrightarrow{(g_1, g_2)} (C_1, C_2) = (A_1, A_2)$$

$$(g_1 \circ f_1, g_2 \circ f_2) \rightarrow (C_1, C_2)$$

Produit direct dans une catégorie

Si A_1, A_2 sont deux objets de $\mathcal{C}$, le système $\langle A, \pi_1, \pi_2 \rangle$ où $A \in \mathcal{C}$ et $\pi_i : A \longrightarrow A_i$ est dit produit direct de A_1 et A_2 si $\forall B \in \mathcal{C}$ et $\forall f_1, f_2$ où $f_i : B \longrightarrow A_i$, il existe un et un seul $f : B \longrightarrow A$ tel que dans le diagramme:

on ait $\pi_i \circ f = f_i$

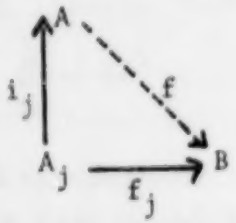
Remarques :

a) on peut montrer que si ce système existe, il est unique et on le note $\langle A_1 \times A_2, \pi_1, \pi_2 \rangle$

b) on peut généraliser à un nombre quelconque de A_i ; le résultat, s'il existe, est noté $\langle \prod A_i, \{\pi_i\}_{i \in I} \rangle$

Somme directe dans une catégorie

Si A_1, A_2 sont deux objets de $\mathcal{B}$, le système $\langle A, i_1, i_2 \rangle$ où $A \in \mathcal{B}$, et i_j : $A_j \longrightarrow A$ est dit somme directe de A_1 et A_2 si $\forall B \in \mathcal{B}$ et $\forall f_1$, f_2 où f_i : $A_i \longrightarrow B$, il existe un et un seul f : $A \longrightarrow B$ tel que dans le diagramme :



on ait $f \circ i_j = f_j$

Remarques :

a) on peut montrer que si ce système existe, il est unique et est noté $\langle A_1 \oplus A_2, i_1, i_2 \rangle$

b) on peut généraliser à un nombre quelconque de A_i ; le résultat, s'il existe, est noté $\langle \bigoplus_{i \in I} A_i, \{i_j\}_{j \in I} \rangle$

Exemples de sommes et produits directs

. Dans la catégorie des Ensembles, le produit direct de A_1 et A_2 est le produit cartésien $A_1 \times A_2$ où

π_i : $A_1 \times A_2 \longrightarrow A_i$ $\qquad$ $\pi_1 (x_1, x_2) = x_1$

$\pi_2 (x_1, x_2) = x_2$

et la somme directe de A_1 et A_2 est l'union disjointe.

. Dans un ensemble ordonné (vu comme catégorie) le produit direct de x_1 et x_2 est inf $\{x_1, x_2\}$ et la somme directe est sup $\{x_1, x_2\}$.

. Il existe des catégories où somme directe ou produit direct n'existent pas.

Morphismes entre les catégories: les FONCTEURS

Comme dans le cas des structures où les morphismes préservent la structure, on voudra définir entre deux catégories un "morphisme" qui préserve la structure de catégories, essentiellement les morphismes identités et l'opération partielle sur les morphismes. Ces "morphismes" seront appelés des foncteurs.

Foncteur

Si $\mathcal{C}$ et $\mathcal{D}$ sont deux catégories, un foncteur de $\mathcal{C}$ à $\mathcal{D}$, $T: \mathcal{C} \longrightarrow \mathcal{D}$, est une double application des objets de $\mathcal{C}$ aux objets de $\mathcal{D}$ et des morphismes de $\mathcal{C}$ aux morphismes de $\mathcal{D}$ telles que:

a) $\forall A \in \mathcal{C} \quad T(1_A) = 1_{T(A)}$

b) $T(gof) = T(g) \circ T(f)$

Explicitement: $A \xrightarrow{1_A} A \Longrightarrow T(A) \xrightarrow{1_{T(A)}} T(A)$

$$A \xrightarrow{f} B \xrightarrow{g} C \Longrightarrow T(A) \xrightarrow{T(f)} T(B) \xrightarrow{T(g)} T(C)$$

($A \xrightarrow{gof} C$; $T(g) \circ T(f) = T(gof)$)

Remarque: on peut définir un autre type de foncteur où la condition b) est remplacée par

b') $T(gof) = T(f) \circ T(g)$

et où $A \xrightarrow{f} B \Longrightarrow T(A) \xleftarrow{T(f)} T(B)$

Exemples de foncteurs

a) $\mathcal{C} \xrightarrow{1_{\mathcal{C}}} \mathcal{C}$ où $1_{\mathcal{C}}(A) = A$ et $1_{\mathcal{C}}(f) = f$ $(f: A \longrightarrow B)$

b) $\mathcal{G} \xrightarrow{\mathcal{O}}$ Ens où $\mathcal{O}(G) =$ G sans opération
$\mathcal{O}(f) =$ f considérée comme application seulement

c) Ens $\xrightarrow{\mathcal{P}}$ Ens où $\mathcal{P}(X) =$ parties de X
$\mathcal{P}(f)$: $\mathcal{P}(A) \longrightarrow \mathcal{P}(B)$ $\quad f: A \longrightarrow B$.

d) Entre deux ensembles ordonnés (ou préordonnés), considérés en tant que catégories, un morphisme pour l'ordre est un foncteur.

Foncteur plein

Un foncteur $\mathcal{C} \xrightarrow{T} \mathcal{D}$ est dit plein si $\forall g$: $T(A) \longrightarrow T(B)$ il existe $f: A \longrightarrow B$ tel que $T(f) = g$.

Foncteur fidèle

Un foncteur $\mathcal{C} \xrightarrow{T} \mathcal{D}$ est dit fidèle si $\forall f_1, f_2: A \longrightarrow B$
$T(f_1) = T(f_2) \Longrightarrow f_1 = f_2$.

Remarques

a) $\mathcal{G} \xrightarrow{\mathcal{O}}$ Ens est fidèle mais pas plein.

b) On peut montrer que si $\mathcal{G} \xrightarrow{T} \mathcal{D}$ est fidèle alors
$T(f)$ monomorphisme $\Longrightarrow f$ monomorphisme
$T(f)$ épimorphisme $\Longrightarrow f$ épimorphisme.

Composition de foncteurs

Si $\mathcal{C} \xrightarrow{F} \mathcal{D} \xrightarrow{H} \mathcal{F}$ sont des foncteurs, on peut définir un nouveau foncteur $\mathcal{C} \xrightarrow{HoF} \mathcal{F}$ en posant:

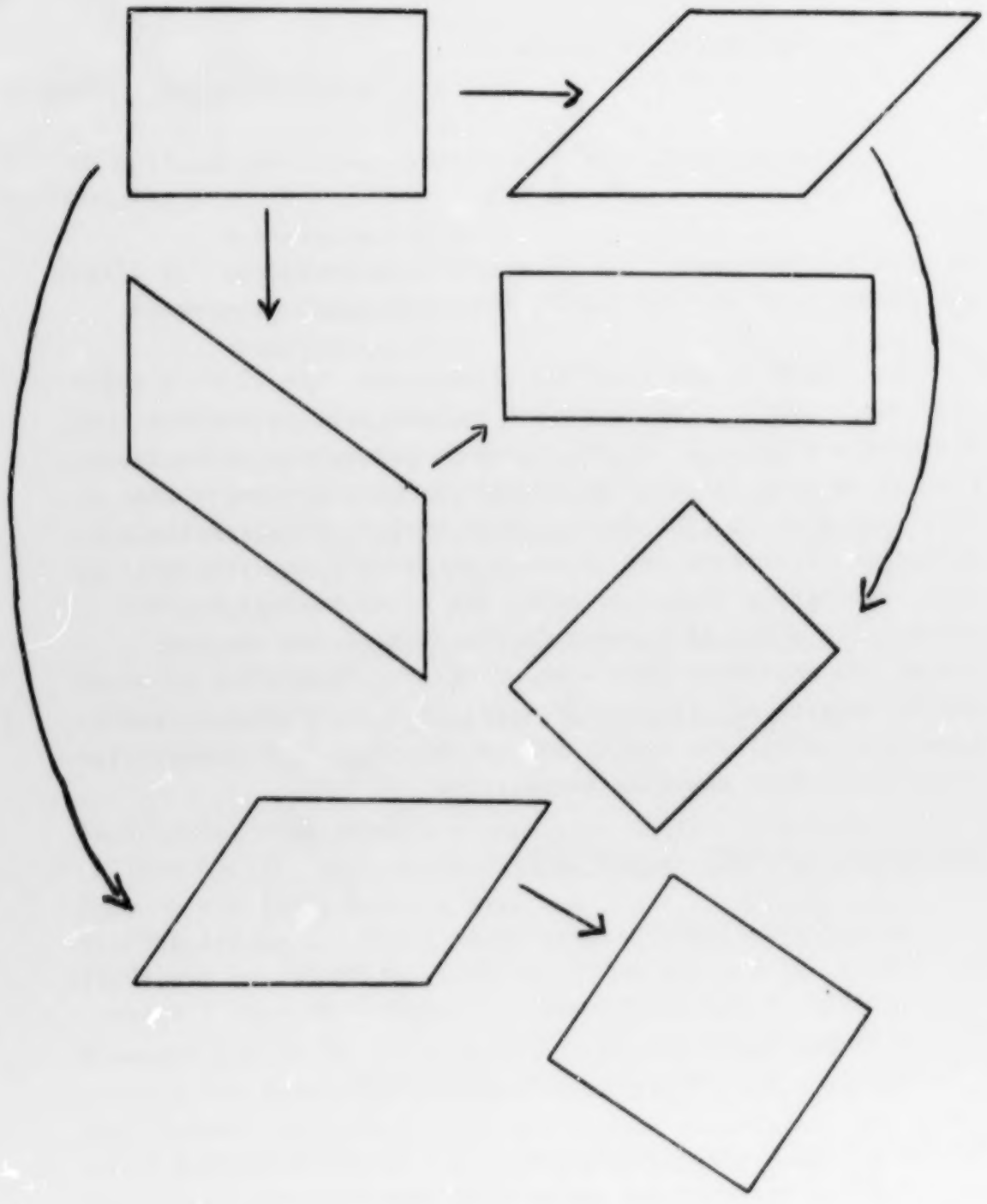
$$(HoF)(A) = H(F(A))$$
$$(HoF)(f) = H(F(f)).$$

On vérifie facilement qu'il s'agit encore d'un foncteur et que cette composition est associative.

§3 Groupements (au sens catégorique)

La notion de groupement a été introduite lors du cours MAT 4823. Il s'agissait de la version de Steiner améliorée (1ère manière) par Wittmann et définie à l'aide de la notion de treillis. Selon cette définition, un groupement était un système $(M, M \times M, \Delta, \circ, \trianglelefteq)$ où M était un ensemble d'états, $M \times M$ un ensemble d'opérations, Δ un sous-ensemble de $M \times M$ d'opérations élémentaires qui "engendrait" $M \times M$ par la loi de composition $(a, b) \circ (b, c) = (a, c)$ et était la <u>couverture</u> de la relation de treillis $\trianglelefteq$. Pour plus de précisions sur cette notion de groupement, on se référera aux notes de cours MAT 4823.

Dans ces notes, on constate que cette définition ne réussit pas à englober toutes les situations envisagées par Piaget ou d'autres situations voisines se présentant dans l'apprentissage de certains concepts. On a des exemples de ce fait aux pages 62 figure 9, 70 et 84 de ce même cours. Nous donnerons plus loin d'autres exemples de telles situations pourtant fort intéressantes du point de vue didactique. Voici pour l'instant une situation tirée de la géométrie. Il s'agit de la conservation d'aires par des cisaillements:



Cette situation ne répond manifestement pas à la définition (1ère manière) de groupement.

Plus simplement, le graphe est:

et ce n'est évidemment pas le graphe d'un treillis. Il s'agit par contre d'un demi-treillis, donc d'un quasi-groupement.

En raison de ces exemples, l'exigence "treillis" s'avère trop restrictive. Une autre des raisons pour lesquelles Wittmann a reformulé la définition de groupement tient dans l'exigence trop restrictive d'avoir au plus une opération élémentaire entre deux états. Nous verrons par la suite des situations intéressantes où cette exigence n'est pas réalisée. Wittmann a choisi le cadre des catégories, à la fois parce qu'il offre de grandes facilités pour décrire des situations englobant plusieurs structures disparates et parce que ce langage met l'accent sur l'aspect important des groupements à savoir les opérations (actions) et leur composition. Voici donc cette nouvelle formulation.

GROUPEMENT (AU SENS CATEGORIQUE)

Un groupement est un quadruplet $(S, T, C, \circ)$ tel que:

G1. $(S, T, \circ)$ est une catégorie où S est constitué des objets (ETATS), T des morphismes (opérations) et $\circ$ est l'opération partielle sur T.
De plus, tout morphisme est inversible.

G2. $C \subseteq T$ et T est engendré par $C \cup C^{-1}$ relativement à $\circ$.
C est l'ensemble des opérations élémentaires.

En d'autres mots, $(S, T, C, \circ)$ est un groupement si $(S, T, \circ)$ est un groupoïde et si T est engendré par $C \cup C^{-1}$.

Remarques sur cette définition

Nous avons les mêmes constituants que dans l'ancienne définition:

S anciennement M
T anciennement M x M
C anciennement Δ
∘ anciennement ∘.

- Mais T n'est plus restreint à S x S. Il peut être de cardinalité plus grande ou plus petite. Autrement dit, il peut y avoir plus d'une opération entre deux états ou même aucune. Il doit cependant être encore engendré par $C \cup C^{-1}$, c'est-à-dire que
  $f \in T \Rightarrow f = f_1 \circ \ldots \circ fn$ où $f_i \in C \cup C^{-1}$ et où C^{-1} désigne les morphismes inverses des morphismes de C.

- Un morphisme est plus dynamique pour représenter une opération qu'un couple.

- La relation binaire ◁ de l'ancienne définition aurait pu être incluse dans celle-ci: Wittmann ne l'a pas fait pour ne pas lui imposer d'être une relation de treillis. Elle sera cependant introduite plus loin pour classifier les types de groupements.

- Demander que (S, T, ∘) soit une catégorie n'est pas nouveau par rapport à l'ancienne définition, puisque cela demande essentiellement que ∘ soit associative et que T contienne toutes les unités, conditions remplies implicitement dans l'ancienne définition. Il en est de même pour l'exigence que tout morphisme soit inversible, puisque dans M x M, pour tout couple (a, b), il y a aussi (b, a).

Suite à ces remarques, vérifions explicitement que cette nouvelle définition englobe l'ancienne.

Soit $(M, M \times M, \Delta, \circ, \measuredangle)$ un groupement (cf MAT 4823, p. 37).

a) Nous avons à vérifier que $(M, M \times M, \circ)$ est une catégorie

M sera notre ensemble d'objets, les éléments de $M \times M$ seront nos morphismes; (a, b) sera le seul morphisme de a à b.

La loi $(a, b) \circ (b, c) = (a, c)$ répond aux conditions de la loi de composition dans une catégorie.

De plus C_1 est vérifié puisque

$$(a, b) = (c, d) \Longleftrightarrow a = c \text{ et } b = d$$

de même que C_2:

$((a, b) \circ (b, c)) \circ (c, d) = (a, c) \circ (c, d) = (a, d)$
$= (a, b) \circ (b, d) = (a, b) \circ ((b, c) \circ (c, d))$.

Enfin chaque objet a possède un morphisme unité qui est
$(a, a) \circ (a, b) = (a, b)$
$(c, a) \circ (a, a) = (c, a)$.

b) Nous avons aussi à vérifier que tout morphisme est inversible

Soit (a, b) un morphisme; alors (b, a) est son inverse car $(a, b) \circ (b, a) = (a, a)$.

c) Il nous reste à vérifier que $M \times M$ est engendré par $\Delta \cup \Delta^{-1}$. Mais ceci est partie de la définition.

Moyens pratiques de reconnaître si un graphe donne lieu à un groupement

Vérifier à chaque cas si la définition catégorique de groupement s'applique peut s'avérer pénible si l'on n'est pas

familier avec la notion de catégorie. Dans certaines situations complexes (par exemple, lorsque la représentation par graphe n'est pas possible) le seul recours demeurera le retour à la définition. Cependant, la plupart du temps, des vérifications plus simples suffisent. Nous allons tenter ici de les mettre en évidence.

Il est essentiel, en premier lieu, de bien identifier ce que seraient S, T et C; dans le cas des graphes, l'opération est toujours du type $(a, b) \circ (b, c) = (a, c)$.

Dans le cas des graphes, les notions catégoriques se traduisent en termes de relations:

* Loi du type $M(A, B) \times M(B, C) \longrightarrow M(A, C)$	transitivité du graphe $(a, b) \circ (b, c) = (a, c)$
associativité de $\circ$	automatique dans un graphe transitif
axiome C_1	automatique par définition du produit cartésien: $(a, b) \neq (a', b')$ si $a \neq a'$ et $b \neq b'$
axiome C_3	graphe réflexif
** tout morphisme est inversible	graphe symétrique
$C \cup C^{-1}$ engendre T	la fermeture symétro-transitive du graphe C est égale au graphe T (résultat de * et **).

Le problème de vérification peut se présenter sous deux formes:

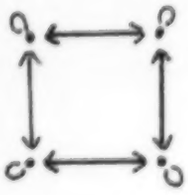
a) on connaît S, T et il faut trouver C ou vérifier si le C donné convient;
b) on connaît S, C et il faut trouver T ou vérifier si le T donné convient.

Dans le 1er cas, il faut d'abord vérifier si (S, T, ∘) forme une catégorie où tous les morphismes sont inversibles. D'après notre dictionnaire précédent, il suffit donc de vérifier si le graphe est une relation d'équivalence (i.e. réflexif, symétrique, transitif). Si c'est le cas, il reste à trouver un C ou à vérifier si le C donné engendre T. D'après notre dictionnaire, il suffit que C soit la couverture symétro-transitive de T.

Dans le second cas, il faut trouver T, ou vérifier si le T donné est tel que (S, T, C, •) est un groupement. Le T devant être engendré par C, il faut donc d'après notre dictionnaire prendre la fermeture symétro-transitive de C et vérifier si le résultat est réflexif (condition manquante pour une relation d'équivalence) et égal à T.

Illustrations

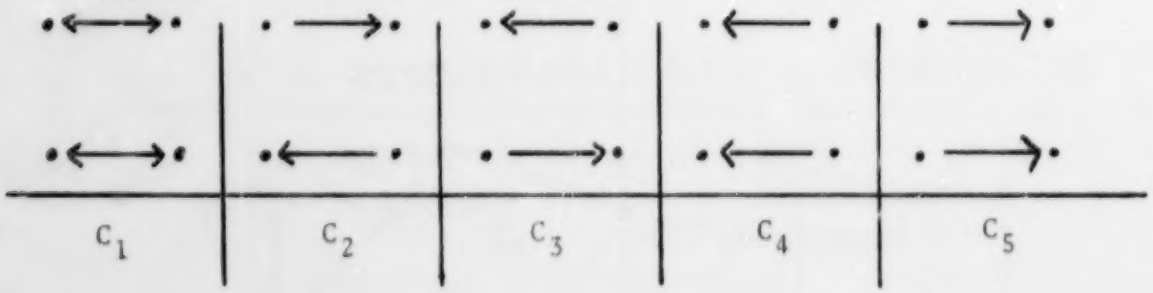
1.1 Soit (S, T, •) comme suit:



Comme ce n'est pas le graphe d'une relation d'équivalence, il est inutile de chercher un C (opérations élémentaires); ce ne peut être un groupement en aucune façon.

1.2 Soit (S, T, ∘) comme suit:

Ceci est le graphe d'une relation d'équivalence. Cherchons alors un C qui engendre T par fermeture symétro-transitive. Il existe en général plusieurs graphes partiels satisfaisant cette condition, chacun donnant lieu à un groupement distinct sur le plan mathématique, mais pouvant se confondre du point de vue conceptuel. En voici quelques-uns:

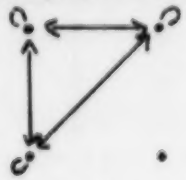


Ainsi, (S, T, C_1, ∘), (S, T, C_2, ∘), (S, T, C_3, ∘), (S, T, C_4, ∘), (S, T, C_5, ∘) sont autant de groupements.

2.1 Soit (S, C, ∘) comme suit:

(C)

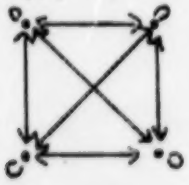
la fermeture symétro-transitive sera



(T)

Ceci n'étant pas le graphe d'une équivalence (S, T, C, ∘) n'est pas un groupement.

2.2 Soit (S, T, C, ∘) comme suit:



(T)

(C)

visiblement, la fermeture symétro-transitive de C ne donne pas T, et ainsi, (S, T, C, ∘) n'est pas un groupement.

§4 Exemples de groupements

4.1 Tout groupe est constituant d'un groupement

En effet, tout groupe (G, •) est groupoïde:

S = {e}

T = G (morphismes inversibles)

∘ = •.

Il suffit de prendre C ⊆ G, un ensemble de générateurs de G.

Ainsi:

$(\{R_0\}, Mc, \{R_{90}, S_A\}, \bullet)$ Mc = Mouvements du carré

$(\{0\}, \mathbb{Z}, \{1\}, +)$

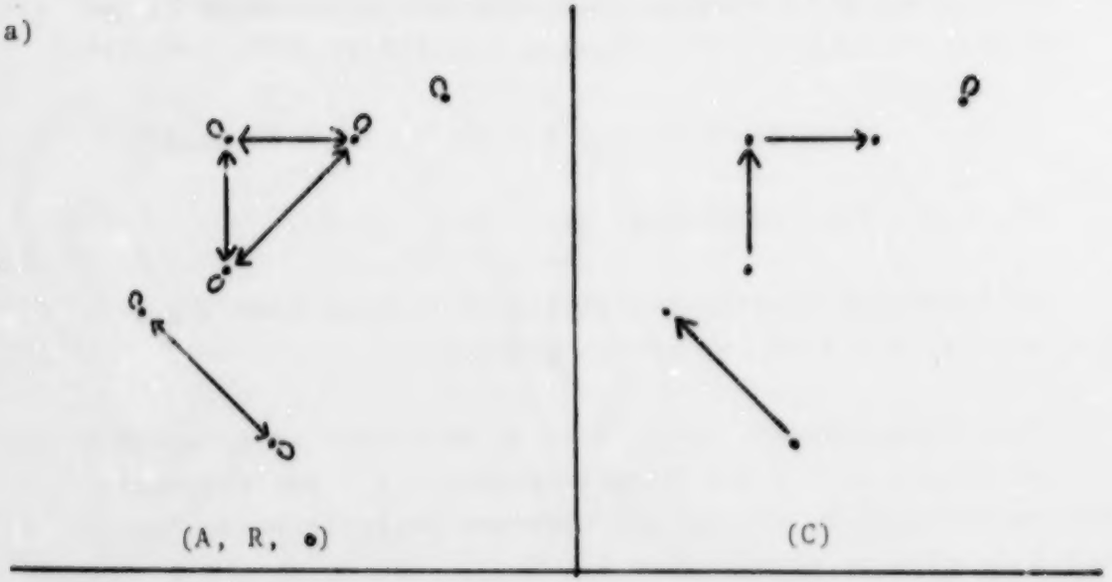
({•}, {Entiers pairs}, {2}, +)

sont des groupements.

4.2 Tout ensemble muni d'une relation d'équivalence (A, R) est constituant d'un groupement

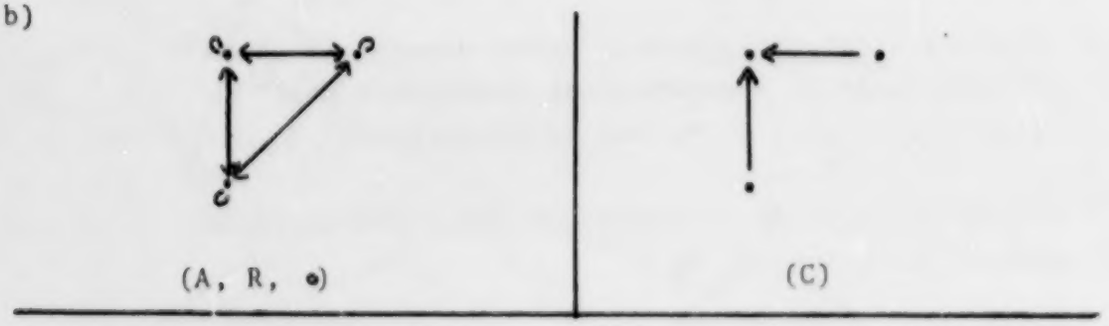
En effet, (A, R) est un ensemble pré-ordonné et est donc une catégorie (cf. p. 81). De plus, tous les morphismes sont inversibles (symétrie de R). Enfin, on peut prendre pour C tout sous-ensemble de R dont la fermeture symétro-transitive donne R.

a)



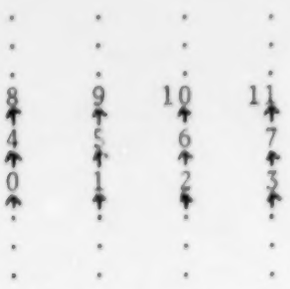
(A, R, •) (C)

b)



(A, R, •) (C)

c) Prenons sur $\mathbb{Z}$ la relation: "diffère par un multiple de 4" (R).
Prenons pour $C \subseteq R$ $C = \{(a, a + 4) \mid a \in \mathbb{Z}\}$ (signifie: "4 de plus").



(C)

La fermeture symétro-transitive de ce graphe donne R et ainsi (Z, R, C, •) est un groupement.

d) Prenons sur $\mathbb{Z}$ la relation "diffère par un multiple de 1" ou si l'on veut $\mathbb{Z} \times \mathbb{Z}$. Prenons $C \subseteq \mathbb{Z} \times \mathbb{Z}$:

$$C = \{(a, a + 1) \mid a \in \mathbb{Z}\} \qquad \text{("1 de plus")}$$

$$\ldots \longrightarrow -1 \longrightarrow 0 \longrightarrow 1 \longrightarrow 2 \longrightarrow \ldots \qquad (C).$$

La fermeture symétro-transitive de C donne bien $\mathbb{Z} \times \mathbb{Z}$ et ainsi $(\mathbb{Z}, \mathbb{Z} \times \mathbb{Z}, C, \bullet)$ est un groupement.

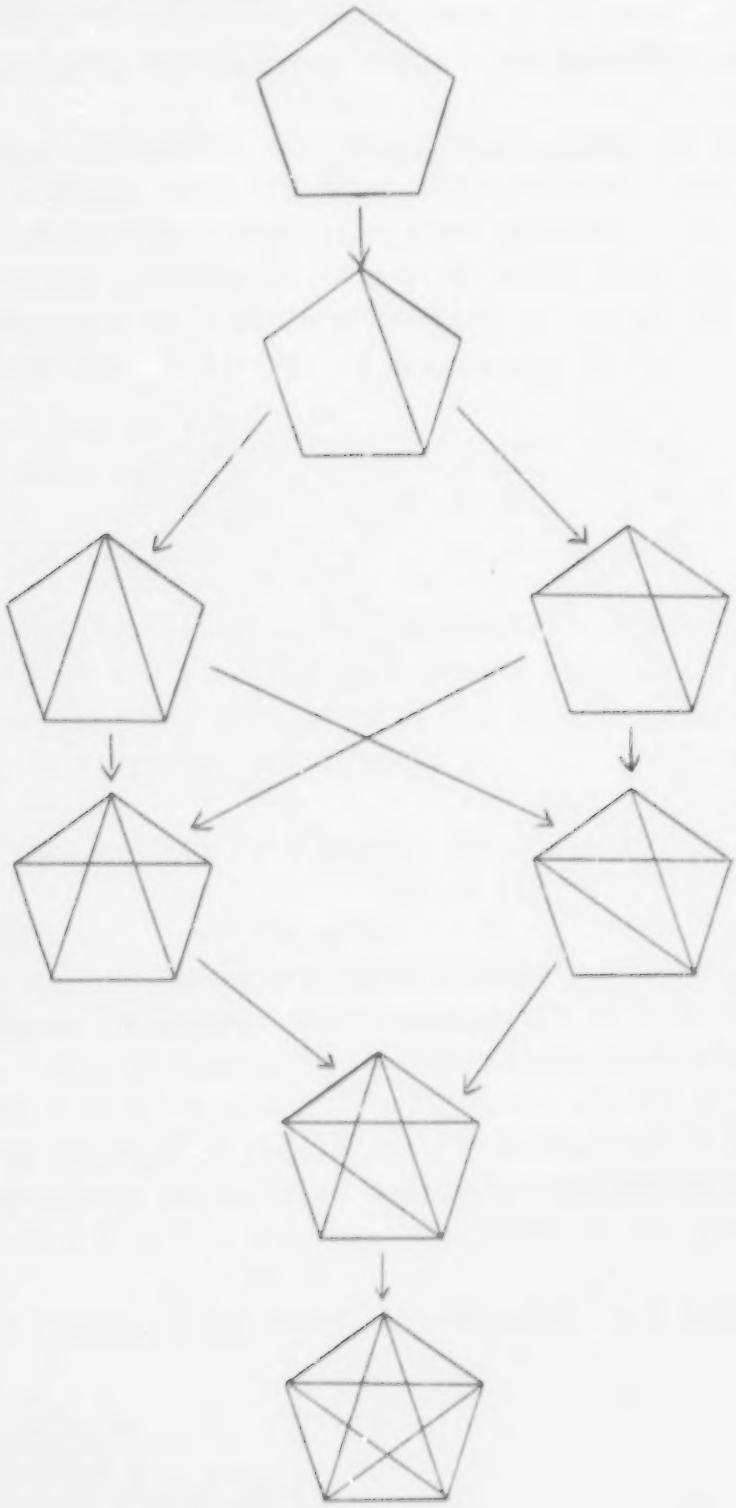
Plus généralement, $(S, S \times S, \bullet)$ deviendra un groupement si l'on trouve un $C \subseteq S \times S$ qui engendre $S \times S$ par fermeture symétro-transitive, ce qui est toujours possible puisqu'on peut à la rigueur prendre $C = S \times S$.

4.3 Prenons L (blocs logiques) comme ensemble d'états. Prenons pour C: "possède une différence avec" alors $(L, L \times L, C, \bullet)$ est un groupement.

Toute relation de différence R sur L procurera un groupement $(L, L \times L, R, \bullet)$.

Toute relation de différence R sur un ensemble A procurera un groupement $(A, T, R, \bullet)$ si T est la fermeture symétro-transitive de R.

4.4 Décompositions successives d'un pentagone régulier (cf. MAT 4823 p. 83).



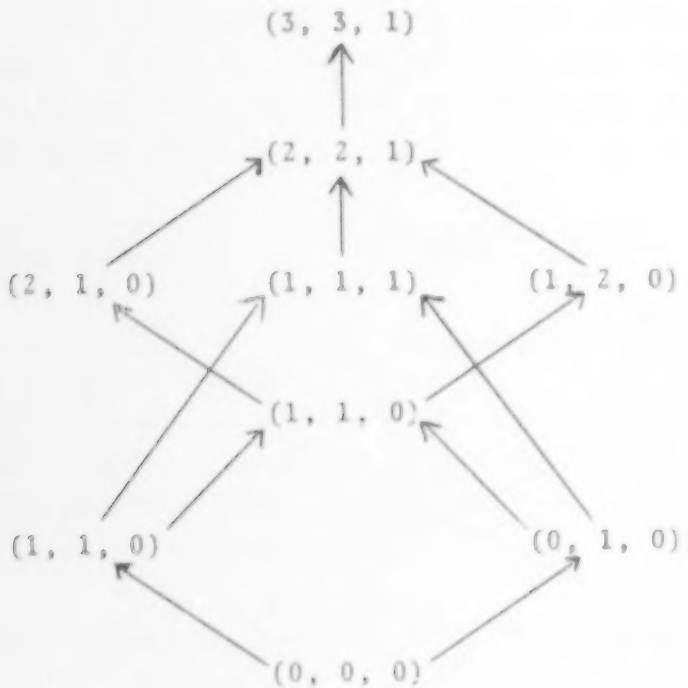
à isométrie près.

(C)

(D, D x D, C, ∘) est un groupement.
D = ensemble des décompositions possibles.

4.5 Composition d'hexaèdres. (cf. MAT 4823 p. 61 et 62).

Considérons le graphe suivant:



Les états S sont les classes d'hexaèdres caractérisés par les critères: nombre de faces parallèles, nombre de quadruplets d'arêtes parallèles et prisme-non prisme.

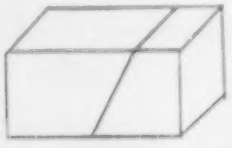
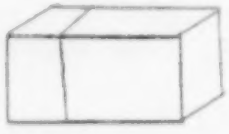
Les flèches C (opérations élémentaires) signifient qu'il existe une façon de composer deux hexaèdres d'une classe pour obtenir un hexaèdre de l'autre classe.

T sera la fermeture symétro-transitive de C. Ici T = S x S.

Ainsi (S, S x S, C, ∘) est un groupement.

Pourtant ce n'est pas un groupement au sens ancien puisque C ne définit pas la couverture d'une relation de treillis.

Si l'on raffine le sens des flèches pour signifier une façon de composer deux hexaèdres afin d'obtenir un nouvel hexaèdre, on obtient alors plus d'une flèche entre certaines paires d'états. Ainsi, il existe au moins deux façons distinctes de composer deux hexaèdres de la classe (2, 2, 1) pour obtenir un hexaèdre de la classe (3, 3, 1):

 ou  ∈ (3, 3, 1)

Bien que le C serait à déterminer avec précision, on voit cependant que le T engendré serait tel que sa cardinalité serait plus grande que celle de S x S et que le résultat (S, T, C, ∘) serait un groupement.

4.6 Les "mots" français à partir des syllabes

Prenons pour ensemble d'états, M, les "mots" français, pour C: "passer d'un mot à un autre en ajoutant à la fin du premier une syllabe".

Alors T = M x M et (M, M x M, C, ∘) est un groupement.

Cependant, C n'est pas la couverture d'une relation de treillis (pas toujours de sup).

Si on ne précise pas où la syllabe est ajoutée (avant ou après), la cardinalité de T dépasse celle de M x M. Exemple:

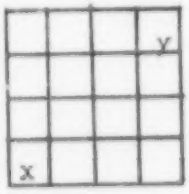
4.7 Un arbre généalogique est constituant d'un groupement. Un des buts d'un tel groupement peut être l'apprentissage des liens de parenté.

"Etre cousin de" donne lien à un groupement où le C n'est pas la couverture ni d'un treillis ni même d'un ordre.

4.8 Nombreux exemples de groupements en arithmétique ou combinatoire. (cf. travaux des étudiants).

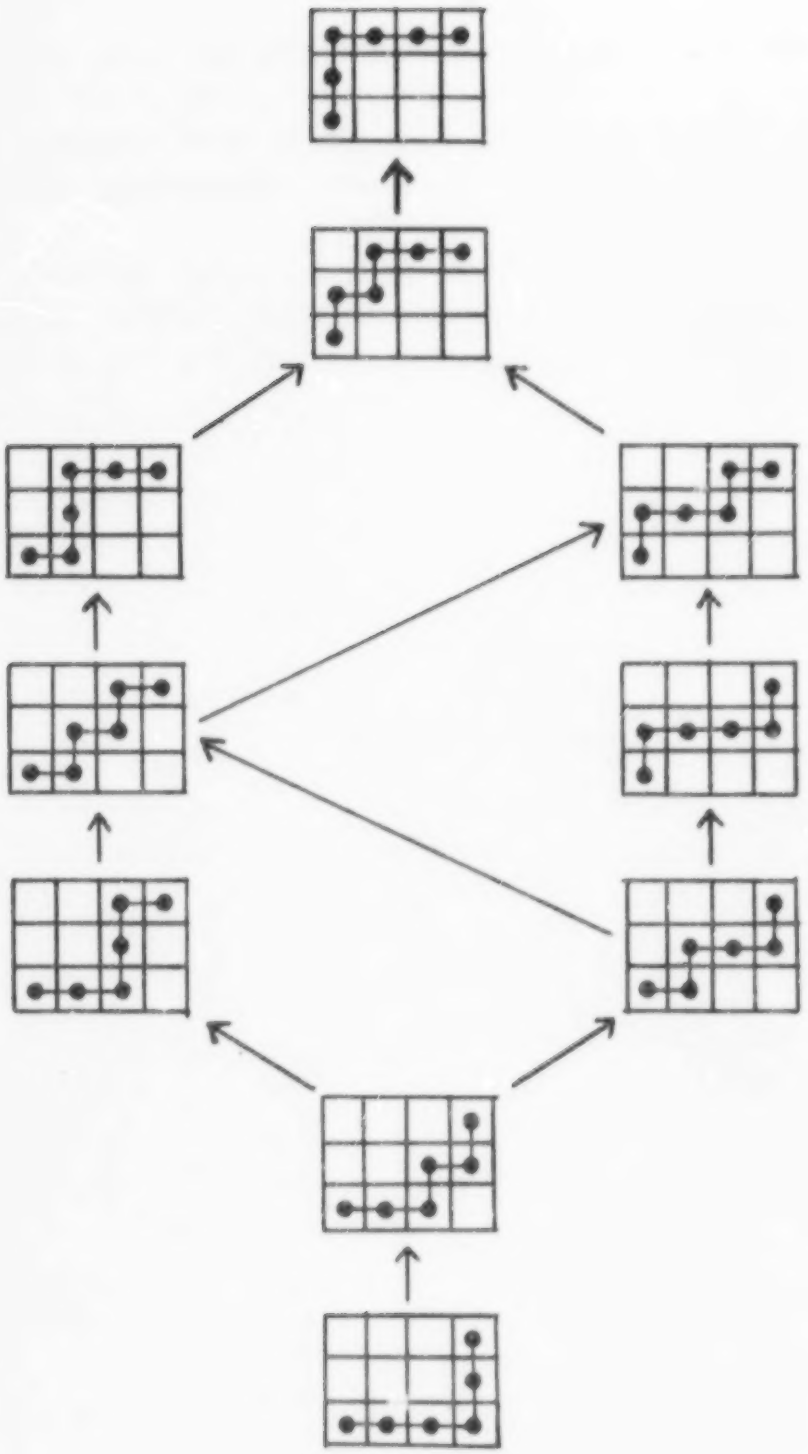
4.9 Chemins menant d'un point à un autre dans un quadrillage.

Considérons le quadrillage.



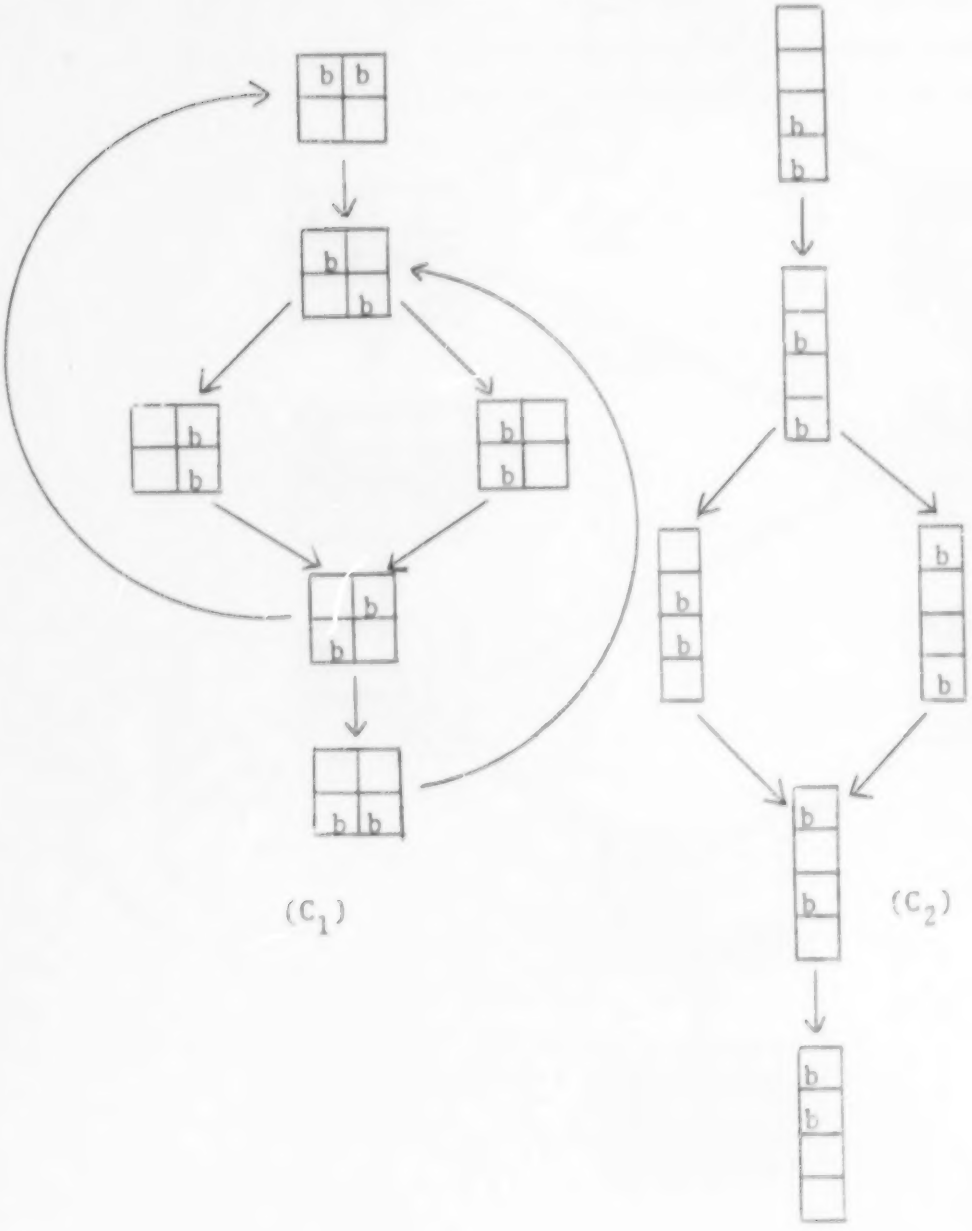
Les états (S) seront les divers chemins conduisant de x à y si les seuls mouvements possibles sont 1 pas vers la droite ou 1 pas vers le haut.

Les opérations élémentaires (C) seront de passer d'un chemin à un autre en ne modifiant que deux mouvements. Voici le graphe de C:



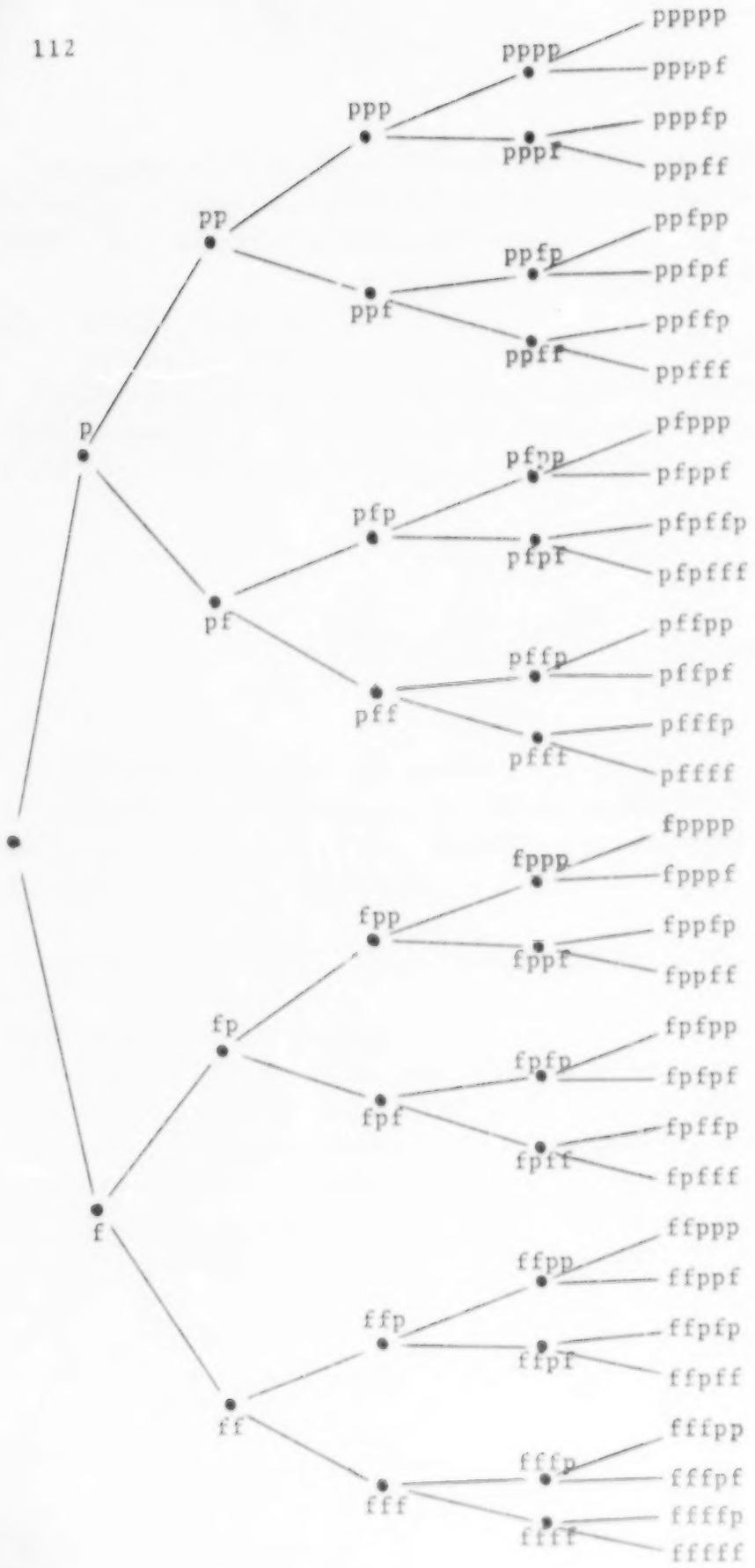
Ainsi (S, S x S, C, o) est un groupement.

4.10 Nombre de façons d'avoir 2 objets de même couleur parmi 4. Prenons des blocs de couleurs (polymaths). Deux façons de les représenter:



Si l'on identifie les états et les morphismes (foncteurs?), on constate que C_1 et C_2 engendrent le même T. Bien que C_1 ne soit pas minimal, il a un intérêt pédagogique puisqu'il ne correspond pas aux mêmes actions concrètes.

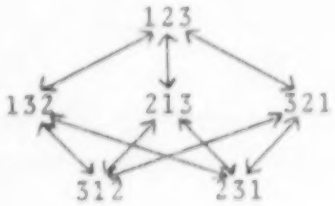
4.11 Après avoir joué à pile ou face 5 fois, quelle est la chance d'avoir obtenu trois piles? Voyons comment l'analyse de ce problème mène à la formation d'un groupement.


pppppp
ppppf
pppp
pppfp
pppf
pppff
ppp
ppfpp
ppfpf
ppfp
ppfff
pp
ppfpp
ppfpf
ppfp
ppfff
ppf
ppfff
ppffp
ppfff
p
pfppp
pfppf
pfpp
pfpfp
pfpf
pfpfff
pfp
pfpfp
pfpf
pfpfff
pf
pffpp
pffpf
pffp
pffff
pff
pffff
pfffp
pffff
pfff
pfffp
pffff
pffff
fpppp
fpppf
fppp
fppfp
fppf
fppff
fpp
fpfpp
fpfpf
fpfp
fpfff
fpf
fpfff
fpffp
fpfff
fpff
fpffp
fpfff
fpfff
fppp
ffppf
ffpp
ffpfp
ffpf
ffpff
ffp
fffpp
fffpf
fffp
ffffp
ffff
ffffp
fffff
ffff
fffp
ffffp
fffff
fff

C est constitué des flèches qui signifient "indiquer le résultat possible après avoir tiré à pile ou face. Les états sont les résultats auxquels on aboutit.

4.12 Permutations de 3 objets

Partons de 123 comme position initiale. Les actions élémentaires (C) seront "permuter deux objets", les états seront les arrangements auxquels on parvient.



(relation de différence!)

On pourrait aussi interpréter les objets 1, 2, 3 comme les sommets d'un triangle. Les permutations de 2 objets seront alors les trois symétries possibles. Les composés de deux flèches seront les rotations.

Nous avons manifestement un groupement possible.

4.13 Une théorie axiomatique est en quelque sorte un groupement, où les états sont les propositions vraies (axiomes et théorèmes) auxquelles on ajoute les définitions et où les actions élémentaires consistent à utiliser tel état dans la démonstration de tel autre état! Une théorie axiomatique est alors un groupement en perpétuelle formation! ("fragment" de groupement).

§5 Classification et représentations réduites de groupements selon Wittmann (1975)

Dans son article de 1975, Wittmann, après avoir donné la définition catégorique de groupement, réintroduit la relation binaire $\trianglelefteq$ qui apparaissait dans l'ancienne définition et l'utilise pour classifier les groupements. Nous allons pour notre part étendre cette classification en nous basant sur les exemples rencontrés à la section précédente.

Définition 1

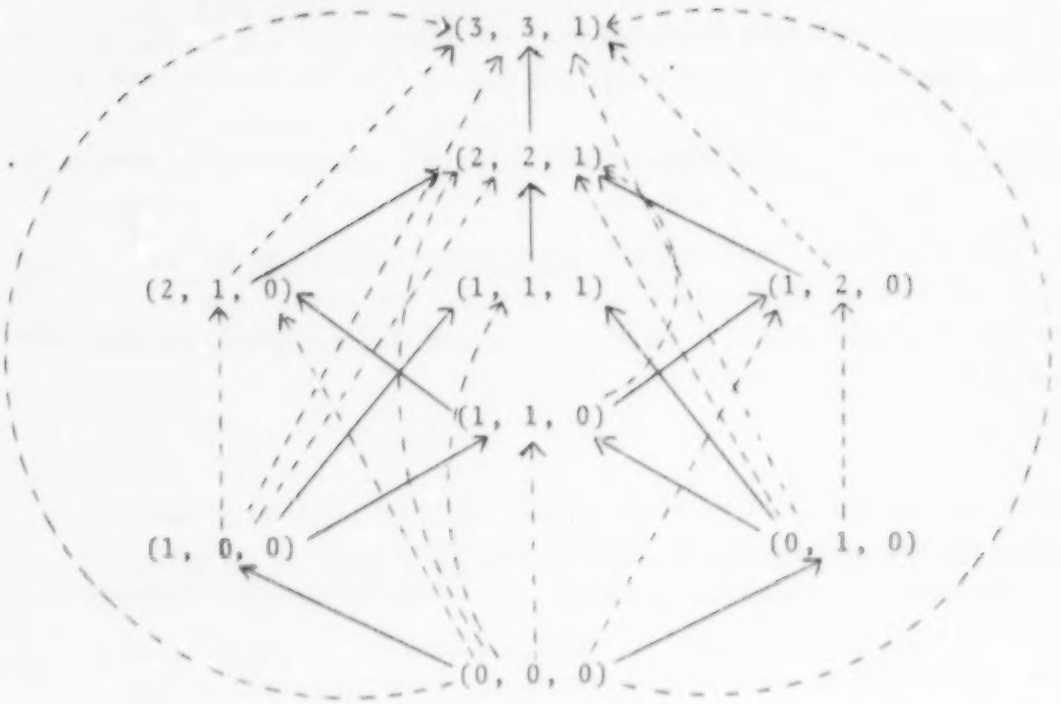
Soit (S, T, C, o) un groupement. $\trianglelefteq$ sera une relation binaire sur S ($\trianglelefteq \subseteq S \times S$) définie comme suit:

$\alpha \trianglelefteq \beta \Longleftrightarrow \exists t \in T$, $t: \alpha \longrightarrow \beta$, et $c_1, \ldots, c_n \in C$ tels que $t = c_1 \circ c_2 \circ \ldots \circ c_n$.

Exemple:

Prenons le groupement 4.5. Appelons H l'ensemble des états. Il s'agit alors du groupement $(H, H \times H, C, \circ)$ où C est représenté par le graphe donné.

Le graphe de $\trianglelefteq$ sera alors:



ce qui est une relation d'ordre mais non de treillis.

Définition 2

(S, T, C, $\circ$, $\trianglelefteq$) est appelé groupement ordonné (respectivement de treillis) si (S, T, C, $\circ$) est un groupement et si $\trianglelefteq$ est une relation d'ordre (respectivement de treillis).

Définition 3

(S, T, C, $\circ$, $\trianglelefteq$) est appelé groupement partiellement ordonné (respectivement totalement ordonné) si (S, T, C, $\circ$) est un groupement et si $\trianglelefteq$ est un ordre partiel (respectivement total).

Définition 3

(S, T, C, $\circ$, $\trianglelefteq$) est appelé groupement d'"équivalence" si (S, T, C, $\circ$) est un groupement et si $\trianglelefteq$ est une équivalence.

Remarque: T est alors engendré par C.

Définition 4

(S, T, C, $\circ$, $\trianglelefteq$) est appelé groupement pré-ordonné si (S, T, C, $\circ$) est un groupement et si $\trianglelefteq$ est un pré-ordre (c'est-à-dire transitif). Tout groupement est un groupement pré-ordonné.

Remarque

D'après la définition même de $\trianglelefteq$, $\trianglelefteq$ est tout simplement la fermeture transitive de C ($\overline{C}$) lorsqu'il s'agit d'un groupement représentable par un graphe.

Une autre façon qu'utilise Wittmann pour classifier les groupements est de considérer la nature de T:

Définition 5 Groupement cartésien

Un groupement (S, T, C, $\circ$) est appelé groupement cartésien si $\forall(\alpha, \beta) \in S \times S$, il existe exactement un morphisme de α à β, t: $\alpha \longrightarrow \beta$.

On peut dans ce cas identifier T à S x S.

D'après l'ancienne définition, les seuls groupements considérés étaient les groupements cartésiens.

Illustrations des définitions précédentes

Pour justifier les définitions précédentes, nous avons à montrer par des exemples qu'elles ne sont pas vides.

Groupement partiellement ordonné (non de treillis):

p. 89, 97 c), exemples 4.4, 4.5, 4.9, 4.10 (C_2), 4.11, 4.7 en prenant "est fils de" comme C. Et alors $\triangleleft$ signifie "est descendant de".

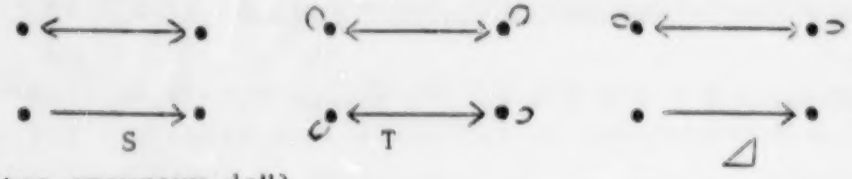
Groupement totalement ordonné (de treillis):

4.2 d).

Groupement d'équivalence:

4.10 (C_1)
4.12, 4.3.

Groupement pré-ordonné:



("être amoureux de")

Groupement non-cartésien:

4.1
4.6 modifié
4.5 raffiné

Représentations réduites de groupements

Wittmann dans son article de 1973 introduit le notion de "groupement interne" qu'il reprend en 1975 sous le nom de "représentation réduite" d'un groupement.

Il s'agit, en gros, de transcrire certains groupements (les groupements cartésiens), lorsque c'est possible, en termes d'une structure algébrique précise, celle de groupe partiel. Ceci permet d'établir un parallèle étroit entre $\trianglelefteq$ et une opération précise. On verra, par exemple, le lien existant entre la relation $\subseteq$ et l'opération $\cup$ (union disjointe), pour les ensembles, entre $\leq$ et $+$ pour les nombres, etc..

Définition de groupe partiel

$(S, +)$ est dit groupe partiel si $+$ est une opération associative partielle possédant un neutre et si les équations $a + x = b$ et $x + a = b$ possèdent une seule solution lorsqu'elle existe.

Exemples de groupes partiels:

5.1 Tout groupe est un groupe partiel.

5.2 $(\mathcal{P}(x), \oplus)$ où $A \oplus B = A \cup B$ si $A \cap B = \emptyset$

5.3 ({bijections de A dans A}, $\circ$)

5.4 $(\mathbb{N}, +)$

Définition de représentation réduite

Soit $(S, S \times S, C, \circ)$ est un groupement (cartésien). S'il existe une opération, notée $+$, sur S telle que $(S, +)$ soit un groupe partiel et que

$$\bullet\ a \trianglelefteq b \Longleftrightarrow \exists s \in S \text{ et } a + s = b\ ;$$

Alors $(S, +)$ est appelé la représentation réduite de $(S, S \times S, C, \circ)$.

Exemples de représentations réduites

5.5 Soit le groupement $(\mathcal{P}(A), \mathcal{P}(A) \times \mathcal{P}(A), \{X \longrightarrow Y \mid |Y| = |X| + 1\}, \circ)$.
Il s'agit du groupement booléen sur les parties de A où les opérations élémentaires correspondent à "un élément de plus".

$\trianglelefteq$ est alors la relation d'inclusion.

La représentation réduite de ce groupement est alors $(\mathcal{P}(A), \oplus)$ où $\oplus$ est l'union disjointe.

En effet $X \subset Y \Longleftrightarrow \exists (Y \setminus X) \in \mathcal{P}(A)$ tel que $X \oplus (Y \setminus X) = Y$.

N.B. Si les opérations élémentaires correspondaient à un élément de moins, $\trianglelefteq$ serait alors la relation $\supseteq$ et la représentation réduite serait alors $(\mathcal{P}(A), \ominus)$ où $X \ominus Y = X \setminus Y$ si $X \supseteq Y$. A rapprocher des remarques du cours 4823 p. 46.

5.6 Soit le groupement $(\mathbb{N}, \mathbb{N} \times \mathbb{N}, \{x \longrightarrow x + 1\}_{x \in \mathbb{N}}, \circ)$.
Ici les opérations élémentaires consistent à ajouter 1.
$\trianglelefteq$ est alors la relation $\leq$.
La représentation réduite de ce groupement est

$$(\mathbb{N}, +)$$

En effet $x \leq y \Longleftrightarrow \exists y - x \in \mathbb{N}$ tel que $x + (y - x) = y$.

5.7 Prenons le groupement 4.6 sur les mots français.

On peut mettre l'opération suivante sur M, l'ensemble des mots français, qui en fait un groupe partiel:

$x_1 \ldots x_n \oplus y_1 \ldots y_n = x_1 \ldots x_n\, y_1 \ldots y_n$

exemple: para $\oplus$ de = parade.

On peut alors facilement vérifier que (M, $\oplus$) est une représentation réduite du groupement 4.6.

Exemple: ra $\rightarrow$ rata $\rightarrow$ rataplan donc ra $\trianglelefteq$ rataplan.

Or ra $\trianglelefteq$ rataplan $\Longleftrightarrow \exists$ taplan $\in$ M tel que ra $\oplus$ taplan = rataplan.

5.8 Prenons le groupement 4.12 (Permutations de 3 objets).

Considérons les objets (états) comme des permutations, P_3, ou mieux comme des bijections particulières de {1, 2, 3}. Ainsi 132 signifie 1 vers 1, 2 vers 3 et 3 vers 2. Munissons P_3 du produit fonctionnel. Alors (P_3, $\circ$) est un groupe partiel qui remplit la condition de représentation réduite pour le groupement initial.

Un exemple de groupement arithmétique

(Les Fractions)

MAT 4883

Louise Aubin

19 avril 1977

Table des matières

1. Analyse mathématique 123

1.1 Présentation des graphes du groupement 123

1.2 Formalisation du groupement 126

1.3 Type de groupement 132

1.4 Interprétation de inf et sup 138

2. Considérations d'ordre didactique 139

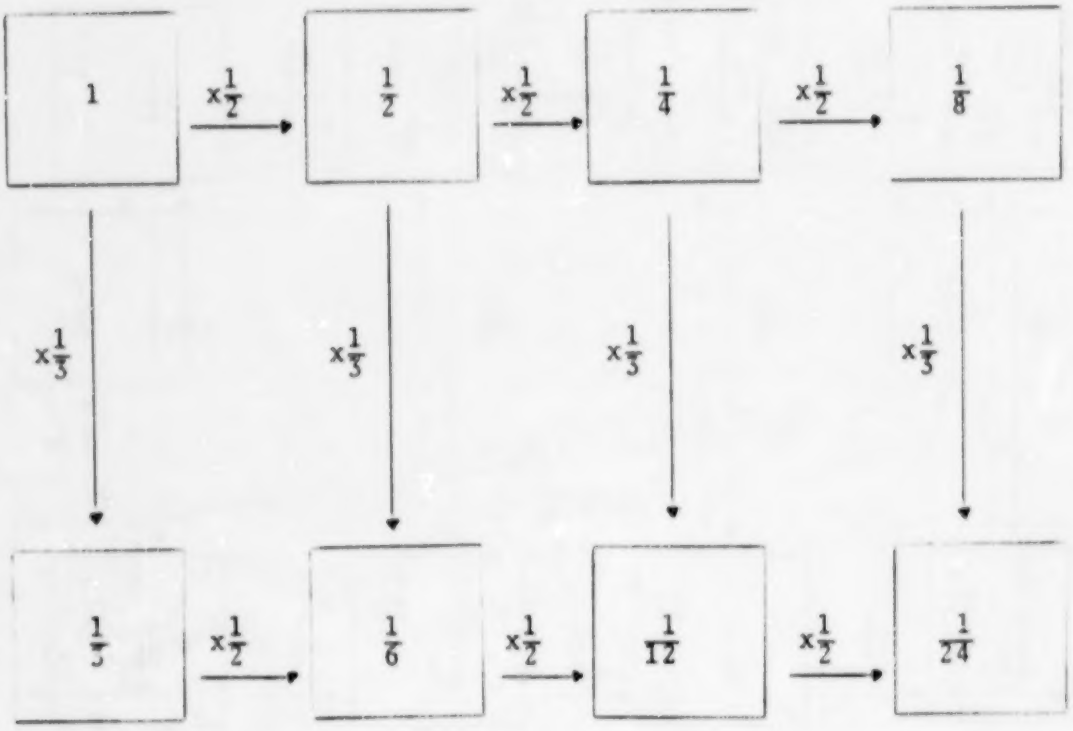
2.1 Aspect dynamique d'un tel groupement 139

2.2 Buts didactiques 141

1. Analyse mathématique du groupement (S, T, C, o)

1.1 Présentation des graphes du groupement (S, T, C, o)

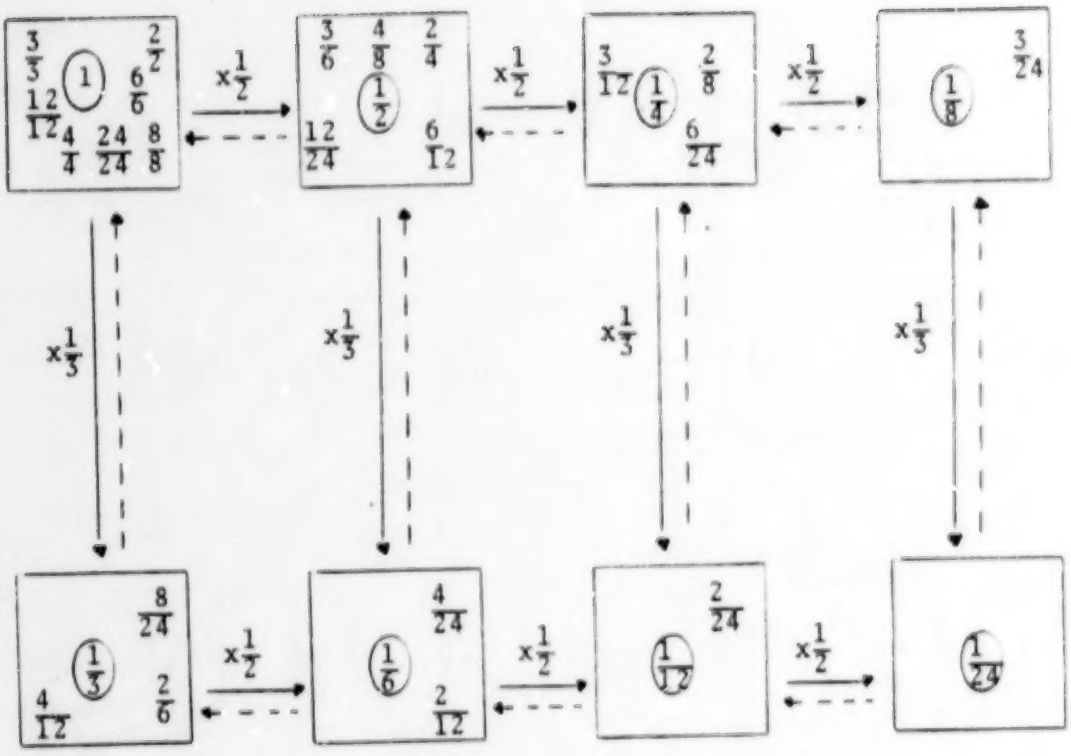
Graphe 1



$S = \{1, \frac{1}{2}, \frac{1}{4}, \frac{1}{8}, \frac{1}{3}, \frac{1}{6}, \frac{1}{12}, \frac{1}{24}\}$

C : $x\frac{1}{2}$ ou $x\frac{1}{3}$ (représenté par les flèches).

Graphe 2



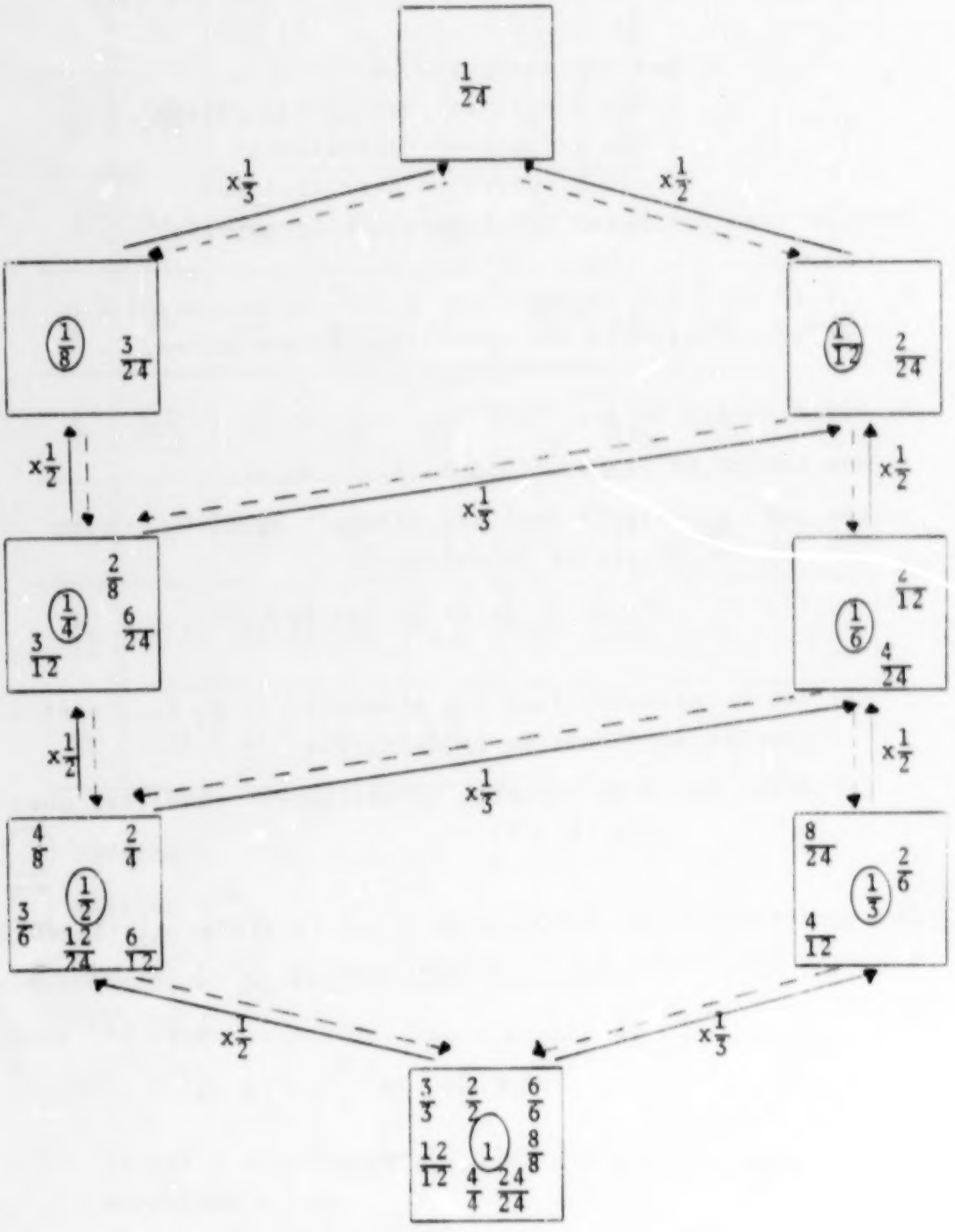
$S = \left\langle 1, \frac{1}{2}, \frac{1}{4}, \frac{1}{8}, \frac{1}{3}, \frac{1}{6}, \frac{1}{12}, \frac{1}{24} \right\rangle$ ensemble d'états engendrés par C.

C : $x\frac{1}{2}$ ou $x\frac{1}{3}$ (représenté par les flèches ⟶)

$S_1 = \left\langle \left[1\right], \left[\frac{1}{2}\right], \left[\frac{1}{4}\right], \left[\frac{1}{8}\right], \left[\frac{1}{3}\right], \left[\frac{1}{6}\right], \left[\frac{1}{12}\right], \left[\frac{1}{24}\right] \right\rangle$ ensemble d'états engendrés par C^{-1} à condition de ne pas réduire la nouvelle fraction formée: Ex: $\frac{1}{24} \times 3 = \frac{3}{24}$

C^{-1}: x2 ou x3 (représenté par les flèches - - ➝)

Une autre présentation du graphe représentant le groupement (S, T, C, o)



1.2 Formalisation du groupement (S, T, C, o)

Un groupement est un quadruplet (S, T, C, o) tel que:

G_1 : (S, T, o) est une catégorie où:
S est constitué des objets (états)
T des morphismes (opérations)
o est l'opération partielle sur T
De plus tout morphisme est inversible (groupoïde)

G_2 : $C \subseteq T$ et T est engendré par $C \cup C^{-1}$ relativement à o.
C'est l'ensemble des opérations élémentaires.

A) Vérification de G_1:

Une catégorie est un triplet (S, T, o) où

-S: est un ensemble dont les éléments A, B, C... sont appelés objets de la catégorie

ici: $S = \left\langle 1, \frac{1}{2}, \frac{1}{4}, \frac{1}{8}, \frac{1}{3}, \frac{1}{6}, \frac{1}{12}, \frac{1}{24} \right\rangle$

-T: est un ensemble dont les éléments f, g, h... sont appelés morphisme de la catégorie

$\forall$(A, B), $\exists$ un ensemble (possiblement vide) tel que:
$M(A, B) \subseteq T$

Je représenterai les éléments de T sur le schéma cartésien qui suit plutôt que sur un schéma sagittal.

T	1	$\frac{1}{2}$	$\frac{1}{4}$	$\frac{1}{8}$	$\frac{1}{3}$	$\frac{1}{6}$	$\frac{1}{12}$	$\frac{1}{24}$
1	x1	(x$\frac{1}{2}$)	x$\frac{1}{4}$	x$\frac{1}{8}$	(x$\frac{1}{3}$)	x$\frac{1}{6}$	x$\frac{1}{12}$	x$\frac{1}{24}$
$\frac{1}{2}$	[x2]	x1	(x$\frac{1}{2}$)	x$\frac{1}{4}$	x$\frac{2}{3}$	(x$\frac{1}{3}$)	x$\frac{1}{6}$	x$\frac{1}{12}$
$\frac{1}{4}$	x4	[x2]	x1	(x$\frac{1}{2}$)	x$\frac{4}{3}$	x$\frac{2}{3}$	(x$\frac{1}{3}$)	x$\frac{1}{6}$
$\frac{1}{8}$	x8	x4	[x2]	x1	x$\frac{8}{3}$	x$\frac{4}{3}$	x$\frac{2}{3}$	(x$\frac{1}{3}$)
$\frac{1}{3}$	[x3]	x$\frac{3}{2}$	x$\frac{3}{4}$	x$\frac{3}{8}$	x1	(x$\frac{1}{2}$)	x$\frac{1}{4}$	x$\frac{1}{8}$
$\frac{1}{6}$	x6	[x3]	x$\frac{3}{2}$	x$\frac{3}{4}$	[x2]	x1	(x$\frac{1}{2}$)	x$\frac{1}{4}$
$\frac{1}{12}$	x12	x6	[x3]	x$\frac{3}{2}$	x4	[x2]	x1	(x$\frac{1}{2}$)
$\frac{1}{24}$	x24	x12	x6	[x3]	x8	x4	[x2]	x1

◯ indique C.

□ indique C^{-1}.

En ordonnée et en abcisse sont les états: S

Dans les cases du schéma, les éléments de T

Ex: M ($\frac{1}{4}$, $\frac{1}{3}$) = x$\frac{4}{3}$ et x$\frac{4}{3}$ ∉ T

N.B. il est à noter que ∀(a, b) il n'y a qu'un seul morphisme a ⟶ b

-o : est une opération partielle sur T du type:

$$M(A, B) \times M(B, C) \longrightarrow M(A, C)$$

si on associe à un morphisme, un couple:

$$M(A, B) \times M(B, C) \longrightarrow M(A, C)$$

$$((a, b) , (b, c)) \longrightarrow (a, c)$$

$$(\tfrac{4}{3}, \tfrac{1}{2}) \longrightarrow \tfrac{2}{3}$$

où

$$\tfrac{2}{3} = \tfrac{4}{3} \times \tfrac{1}{2}$$

Une catégorie doit satisfaire aux axiomes suivants:

C_1: Un morphisme attaché à un couple ne peut être confondu avec un morphisme attaché à un autre couple.

Cet axiome peut être facilement vérifié sur le tableau cartésien p.127. A tout couple, dans cet exemple de groupement, correspond un et un seul morphisme; on ne peut donc confondre un morphisme attaché à un couple avec celui attaché à un autre couple à condition de distinguer, par exemple, $\tfrac{3}{2} \in M(\tfrac{1}{6}, \tfrac{1}{4})$ de $\tfrac{3}{2} \in M(\tfrac{1}{12}, \tfrac{1}{8})$

C_2: L'opération partielle est associative:

$$f \circ (goh) = f \circ (goh)$$

Dans le présent groupement, composer des morphismes revient à multiplier des éléments de Q; et la multiplication dans Q est associative.

Ex: $\frac{1}{2} \xrightarrow{x\frac{1}{2}} \frac{1}{4} \xrightarrow{x\frac{1}{2}} \frac{1}{8} \xrightarrow{x\frac{1}{3}} \frac{1}{24}$ ou $\frac{1}{2} \xrightarrow{x\frac{1}{2}} \frac{1}{4} \xrightarrow{x\frac{1}{2}} \frac{1}{8} \xrightarrow{x\frac{1}{3}} \frac{1}{24}$

$\frac{1}{2} \xrightarrow{x\frac{1}{4}} \frac{1}{8} \xrightarrow{x\frac{1}{3}} \frac{1}{24}$ ou $\frac{1}{2} \xrightarrow{x\frac{1}{6}} \frac{1}{12}$

$(x\frac{1}{2} \quad x\frac{1}{2}) \quad x \frac{1}{3}$ $\qquad$ $x\frac{1}{2} \quad (x\frac{1}{2} \times \frac{1}{3})$

$x\frac{1}{4} \quad x \frac{1}{3}$ $\qquad$ $x\frac{1}{2} \quad x \frac{1}{6}$

$x\frac{1}{12}$ $\qquad = \qquad$ $x\frac{1}{12}$

C_3: Chaque objet A possède un morphisme unité noté I_A.

Ici, le morphisme unité est x1 et apparait sur la diagonale (N.O. - S.E.) du tableau cartésien p. 127.

La preuve que le morphisme unité est x1 repose sur le fait que 1 est l'élément neutre pour la multiplication dans Q.

Ex: $I_A \circ f = f$

$x1 \times \frac{1}{2} = x\frac{1}{2}$

Il reste à vérifier que tout morphisme est inversible.

Il est facile de constater dans le tableau cartésien de T que $\forall$ (A, B), le M(A, B) $\in$ T possède un inverse qui est M (B, A) $\in$ T qui à la propriété suivante

M (A, B) . M (B, A) = IA

Ex: M $(\frac{1}{2}, \frac{1}{4})$. M $(\frac{1}{4}, \frac{1}{2})$ = IA

$x\frac{1}{2}$. x2 = x1

Comme la multiplication dans Q possède un inverse

$(\frac{a}{b})^{-1} = \frac{b}{a}$, le morphisme inverse de $x\frac{a}{b} = x\frac{b}{a}$

B) Vérification de G_2:

$C \subseteq T$ et T est engendré par $C \cup C^{-1}$ relativement à o.

C'est l'ensemble des opérations élémentaires.

1^o $C \subseteq T$: le tableau cartésien en p. 127 illustre cette relation.

2^o Test engendré par $C \cup C^{-1}$ relativement à o:

$\forall \frac{a}{b} \in T$, a|24 et b|24

or, $24 = 2 \times 2 \times 2 \times 3$

Donc a et b s'écrivent en termes de 2 ou de 3.

Ainsi $\frac{a}{b}$ s'écrit en termes de 2 et/ou de 3 ($\in C^{-1}$) et/ou de $\frac{1}{2}$ et/ou de $\frac{1}{3}$ ($\in C$).

Conclusion

G_1 et G_2 étant vérifiés on peut conclure que (S, T, C, o) est un groupement.

Remarques:

On peut remarquer que les états de ce groupement ont été définis ainsi: $S=\left\langle 1, \frac{1}{2}, \frac{1}{4}, \frac{1}{8}, \frac{1}{3}, \frac{1}{6}, \frac{1}{12}, \frac{1}{24} \right\rangle$. Je n'ai pas insisté dans l'analyse mathématique sur le fait que les états peuvent être vus comme des classes de fractions. De toute façon, il est clair, du point de vue mathématique, qu'une fraction est perçue comme un élément d'une classe (rationnel). De plus, la présentation des états considérés comme classes a pour moi, un but davantage didactique que mathématique. D'ailleurs comme on peut le constater les quelques représentants qui apparaissent dans les classes ne sont ceux que le matériel Cuisenaire permet de construire compte tenu de ses limites et du choix de l'unité de base. Exemple: ainsi $\frac{5}{10}$ n'apparaît pas dans $\frac{1}{2}$. Je n'ai donc pas tenu compte des états considérés comme des classes (même si on peut le faire) puisque le fait de les considérer comme fractions me permet de former quand même un groupement intéressant.

1.3 Type de groupement

Le groupement (S, T, C, o) est un groupement cartésien d'ordre partiel et de treillis.

A) Groupement cartésien:

Un groupement (S, T, C, o) est appelé groupement cartésien si $\forall (\alpha,\beta) \in S \times S$, il existe exactement un morphisme de α à β : t : $\alpha \longrightarrow \beta$.

On peut, dans ce cas, "identifier" T à S x S et évidemment #T = #(S x S)

T	1	$\frac{1}{2}$	$\frac{1}{4}$	$\frac{1}{8}$	$\frac{1}{3}$	$\frac{1}{6}$	$\frac{1}{12}$	$\frac{1}{24}$
1	x1	$x\frac{1}{2}$	$x\frac{1}{4}$	$x\frac{1}{8}$	$x\frac{1}{3}$	$x\frac{1}{6}$	$x\frac{1}{12}$	$x\frac{1}{24}$
$\frac{1}{2}$	x2	x1	$x\frac{1}{2}$	$x\frac{1}{4}$	$x\frac{2}{3}$	$x\frac{1}{3}$	$x\frac{1}{6}$	$x\frac{1}{12}$
$\frac{1}{4}$	x4	x2	x1	$x\frac{1}{2}$	$x\frac{4}{3}$	$x\frac{2}{3}$	$x\frac{1}{3}$	$x\frac{1}{6}$
$\frac{1}{8}$	x8	x4	x2	x1	$x\frac{8}{3}$	$x\frac{4}{3}$	$x\frac{2}{3}$	$x\frac{1}{3}$
$\frac{1}{3}$	x3	$x\frac{3}{2}$	$x\frac{3}{4}$	$x\frac{3}{8}$	x1	$x\frac{1}{2}$	$x\frac{1}{4}$	$x\frac{1}{8}$
$\frac{1}{6}$	x6	x3	$x\frac{3}{2}$	$x\frac{3}{4}$	x2	x1	$x\frac{1}{2}$	$x\frac{1}{4}$
$\frac{1}{12}$	x12	x6	x3	$x\frac{3}{2}$	x4	x2	x1	$x\frac{1}{2}$
$\frac{1}{24}$	x24	x12	x6	x3	x8	x4	x2	x1

SxS	1	$\frac{1}{2}$	$\frac{1}{4}$	$\frac{1}{8}$	$\frac{1}{3}$	$\frac{1}{6}$	$\frac{1}{12}$	$\frac{1}{24}$
1	$(1,1)$	$(1,\frac{1}{2})$	$(1,\frac{1}{4})$	$(1,\frac{1}{8})$	$(1,\frac{1}{3})$	$(1,\frac{1}{6})$	$(1,\frac{1}{12})$	$(1,\frac{1}{24})$
$\frac{1}{2}$	$(\frac{1}{2},1)$	$(\frac{1}{2},\frac{1}{2})$	$(\frac{1}{2},\frac{1}{4})$	$(\frac{1}{2},\frac{1}{8})$	$(\frac{1}{2},\frac{1}{3})$	$(\frac{1}{2},\frac{1}{6})$	$(\frac{1}{2},\frac{1}{12})$	$(\frac{1}{2},\frac{1}{24})$
$\frac{1}{4}$	$(\frac{1}{4},1)$	$(\frac{1}{4},\frac{1}{2})$	$(\frac{1}{4},\frac{1}{4})$	$(\frac{1}{4},\frac{1}{8})$	$(\frac{1}{4},\frac{1}{3})$	$(\frac{1}{4},\frac{1}{6})$	$(\frac{1}{4},\frac{1}{12})$	$(\frac{1}{4},\frac{1}{24})$
$\frac{1}{8}$	$(\frac{1}{8},1)$	$(\frac{1}{8},\frac{1}{2})$	$(\frac{1}{8},\frac{1}{4})$	$(\frac{1}{8},\frac{1}{8})$	$(\frac{1}{8},\frac{1}{3})$	$(\frac{1}{8},\frac{1}{6})$	$(\frac{1}{8},\frac{1}{12})$	$(\frac{1}{8},\frac{1}{24})$
$\frac{1}{3}$	$(\frac{1}{3},1)$	$(\frac{1}{3},\frac{1}{2})$	$(\frac{1}{3},\frac{1}{4})$	$(\frac{1}{3},\frac{1}{8})$	$(\frac{1}{3},\frac{1}{3})$	$(\frac{1}{3},\frac{1}{6})$	$(\frac{1}{3},\frac{1}{12})$	$(\frac{1}{3},\frac{1}{24})$
$\frac{1}{6}$	$(\frac{1}{6},1)$	$(\frac{1}{6},\frac{1}{2})$	$(\frac{1}{6},\frac{1}{4})$	$(\frac{1}{6},\frac{1}{8})$	$(\frac{1}{6},\frac{1}{3})$	$(\frac{1}{6},\frac{1}{6})$	$(\frac{1}{6},\frac{1}{12})$	$(\frac{1}{6},\frac{1}{24})$
$\frac{1}{12}$	$(\frac{1}{12},1)$	$(\frac{1}{12},\frac{1}{2})$	$(\frac{1}{12},\frac{1}{4})$	$(\frac{1}{12},\frac{1}{8})$	$(\frac{1}{12},\frac{1}{3})$	$(\frac{1}{12},\frac{1}{6})$	$(\frac{1}{12},\frac{1}{12})$	$(\frac{1}{12},\frac{1}{24})$
$\frac{1}{24}$	$(\frac{1}{24},1)$	$(\frac{1}{24},\frac{1}{2})$	$(\frac{1}{24},\frac{1}{4})$	$(\frac{1}{24},\frac{1}{8})$	$(\frac{1}{24},\frac{1}{3})$	$(\frac{1}{24},\frac{1}{6})$	$(\frac{1}{24},\frac{1}{12})$	$(\frac{1}{24},\frac{1}{24})$

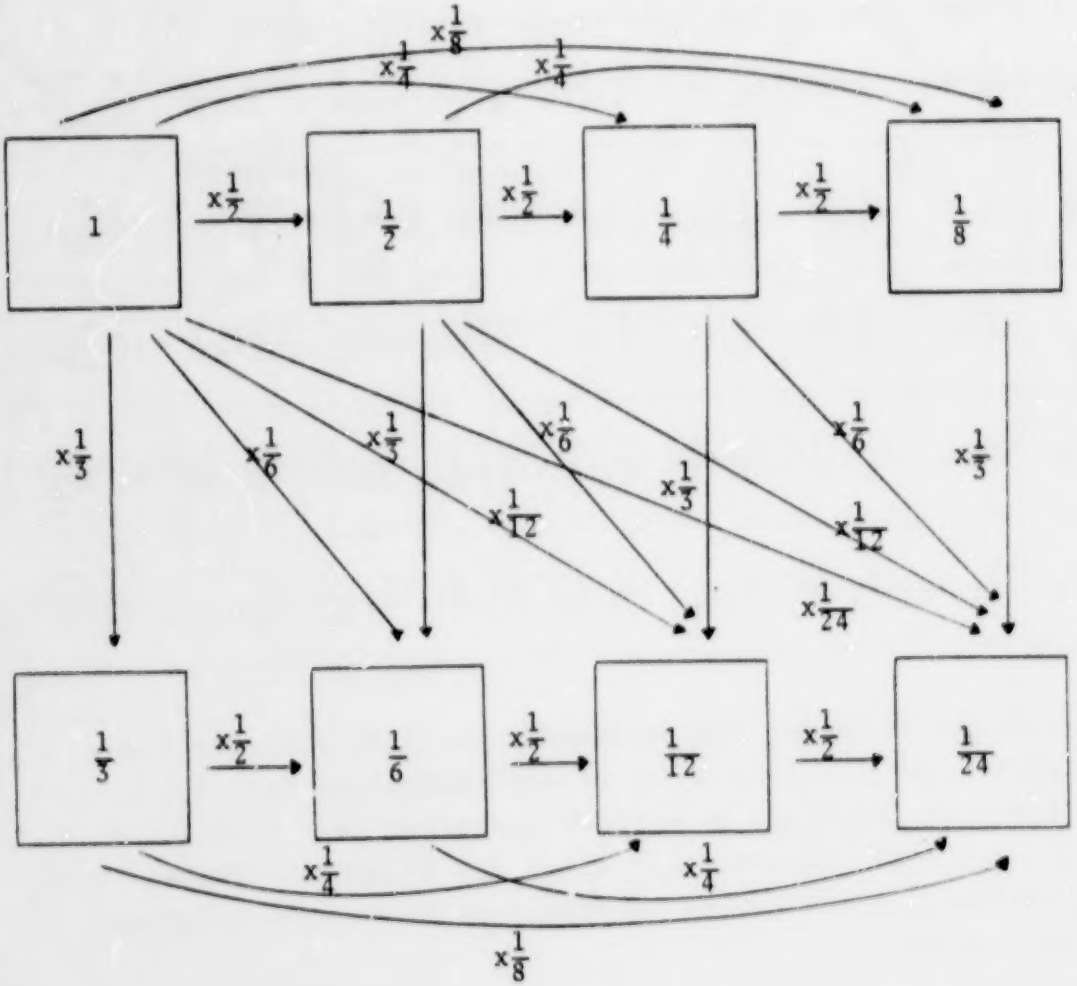
Le tableau cartésien représentant T (p. 132) illustre bien, je pense, qu'il existe un et un seul morphisme de α à β. De plus, en comparant le tableau cartésien de T et celui de S x S (p. 133), on peut voir qu'il est possible d'établir une bijection de $T \longrightarrow S \times S$ en associant un et un seul morphisme à tout couple.

B) Groupement d'ordre partiel:

(S, T, C, o, $\trianglelefteq$) est appelé groupement partiellement ordonné si (S, T, C, o) est un groupement et si $\trianglelefteq$ est un ordre partiel.

Il reste à vérifier que $\trianglelefteq$ est un ordre partiel; $\trianglelefteq$ est défini comme étant la fermeture transitive de C. Le graphe qui suit représente $\trianglelefteq$.

Graphe représentant $\trianglelefteq$: $\frac{1}{a} \trianglelefteq \frac{1}{b} \Longleftrightarrow$ a est facteur de b$(a \neq b)$



Le graphe obtenu est bien celui d'une relation d'ordre (antisymétrie et transitivité se vérifient) et d'ordre partiel car:

$$\exists (a, b) \text{ tel que } a \not\mathcal{R} b \text{ et } b \not\mathcal{R} a$$

c'est-à-dire, il existe au moins une paire inerte;

Ex: $(\frac{1}{3}, \frac{1}{2})$

C) Groupement de treillis:

Un ensemble ordonné est un treillis si $\forall (a, b)$, $\exists a \sqcap b$ = borne inférieure et $a \sqcup b$ = borne supérieure.

Les tableaux suivants montrent que $\forall (a, b) \in S \times S$, on peut associer un élément $a \sqcap b$ et $a \sqcup b$.

$\sqcap$	1	$\frac{1}{2}$	$\frac{1}{3}$	$\frac{1}{4}$	$\frac{1}{6}$	$\frac{1}{8}$	$\frac{1}{12}$	$\frac{1}{24}$
1	1	1	1	1	1	1	1	1
$\frac{1}{2}$	1	$\frac{1}{2}$	1	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$
$\frac{1}{3}$	1	1	$\frac{1}{3}$	1	$\frac{1}{3}$	1	$\frac{1}{3}$	$\frac{1}{3}$
$\frac{1}{4}$	1	$\frac{1}{2}$	1	$\frac{1}{4}$	$\frac{1}{2}$	$\frac{1}{4}$	$\frac{1}{4}$	$\frac{1}{24}$
$\frac{1}{6}$	1	$\frac{1}{2}$	$\frac{1}{3}$	$\frac{1}{2}$	$\frac{1}{6}$	$\frac{1}{2}$	$\frac{1}{6}$	$\frac{1}{6}$
$\frac{1}{8}$	1	$\frac{1}{2}$	1	$\frac{1}{4}$	$\frac{1}{2}$	$\frac{1}{8}$	$\frac{1}{4}$	$\frac{1}{8}$
$\frac{1}{12}$	1	1	$\frac{1}{3}$	$\frac{1}{4}$	$\frac{1}{6}$	$\frac{1}{4}$	$\frac{1}{12}$	$\frac{1}{12}$
$\frac{1}{24}$	1	$\frac{1}{2}$	$\frac{1}{3}$	$\frac{1}{4}$	$\frac{1}{6}$	$\frac{1}{8}$	$\frac{1}{12}$	$\frac{1}{24}$

$\sqcup$	1	$\frac{1}{2}$	$\frac{1}{3}$	$\frac{1}{4}$	$\frac{1}{6}$	$\frac{1}{8}$	$\frac{1}{12}$	$\frac{1}{24}$
1	1	$\frac{1}{2}$	$\frac{1}{3}$	$\frac{1}{4}$	$\frac{1}{6}$	$\frac{1}{8}$	$\frac{1}{12}$	$\frac{1}{24}$
$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{6}$	$\frac{1}{4}$	$\frac{1}{6}$	$\frac{1}{8}$	$\frac{1}{12}$	$\frac{1}{24}$
$\frac{1}{3}$	$\frac{1}{3}$	$\frac{1}{6}$	$\frac{1}{3}$	$\frac{1}{12}$	$\frac{1}{6}$	$\frac{1}{24}$	$\frac{1}{12}$	$\frac{1}{24}$
$\frac{1}{4}$	$\frac{1}{4}$	$\frac{1}{4}$	$\frac{1}{12}$	$\frac{1}{4}$	$\frac{1}{12}$	$\frac{1}{8}$	$\frac{1}{12}$	$\frac{1}{24}$
$\frac{1}{6}$	$\frac{1}{6}$	$\frac{1}{6}$	$\frac{1}{6}$	$\frac{1}{12}$	$\frac{1}{6}$	$\frac{1}{24}$	$\frac{1}{12}$	$\frac{1}{24}$
$\frac{1}{8}$	$\frac{1}{8}$	$\frac{1}{8}$	$\frac{1}{24}$	$\frac{1}{8}$	$\frac{1}{24}$	$\frac{1}{8}$	$\frac{1}{24}$	$\frac{1}{24}$
$\frac{1}{12}$	$\frac{1}{12}$	$\frac{1}{12}$	$\frac{1}{12}$	$\frac{1}{12}$	$\frac{1}{12}$	$\frac{1}{24}$	$\frac{1}{12}$	$\frac{1}{24}$
$\frac{1}{24}$	$\frac{1}{24}$	$\frac{1}{24}$	$\frac{1}{24}$	$\frac{1}{24}$	$\frac{1}{24}$	$\frac{1}{24}$	$\frac{1}{24}$	$\frac{1}{24}$

1.4 Interprétations de inf et sup de $(S, T, C, \circ, \trianglelefteq)$

$$S = \left\langle 1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \frac{1}{8}, \frac{1}{12}, \frac{1}{24} \right\rangle$$

Les états de ce groupement de treillis peuvent être définis en compréhension de la manière suivante:

$$S = \left\langle \frac{a}{b} \in Q \text{ où } a = 1 \text{ et } b \in f(24) \right\rangle \quad f(24) = \langle \text{facteurs de } 24 \rangle$$

N.B.: L'état "1" du groupement pouvant s'écrire sous la forme $\frac{1}{1}$

Interprétation de $\sqcap$:

$$\forall \left(\frac{1}{a}, \frac{1}{b}\right), \inf \left\langle \frac{1}{a}, \frac{1}{b} \right\rangle = \frac{1}{x} \quad \text{où} \quad x = \text{PGCD de a et b}$$

Interprétation de $\sqcup$:

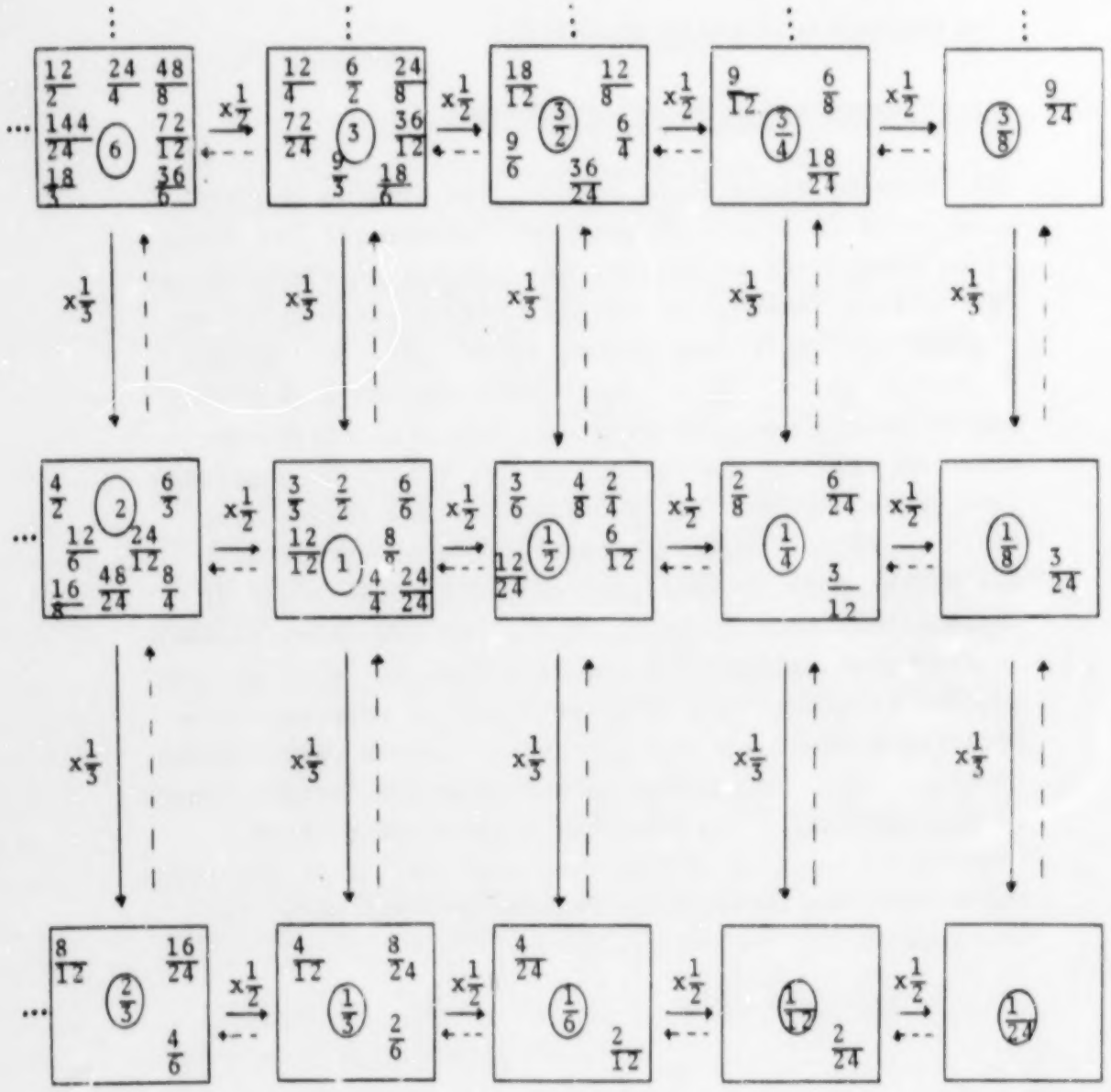
$$\forall \left(\frac{1}{a}, \frac{1}{b}\right), \sup \left\langle \frac{1}{a}, \frac{1}{b} \right\rangle = \frac{1}{x} \quad \text{où} \quad x = \text{PPCM de a et b}$$

2. Considérations d'ordre didactique

2.1 Aspect dynamique d'un tel groupement

Une certaine unité étant donnée, les enfants peuvent construire (à l'aide du matériel Cuisenaire) les états de ce groupement en faisant les opérations élémentaires (prendre la demie ou le tiers). Ils peuvent aussi en faisant les opérations élémentaires inverses (prendre le double ou le triple) "enrichir" les états déjà obtenus et leur donner une signification plus abstraite, celle de classes (rationnel) où les fractions apparaissent comme éléments de ces classes. Les seules fractions qu'il est toutefois possible de découvrir avec une telle unité de base sont celles où numérateur et dénominateur sont facteurs de 24. De nouvelles classes de fractions (illustrées par le graphe qui suit p. 140) peuvent éventuellement être obtenues en refaisant l'opération élémentaire sur certaines classes déjà formées (voir p. 140). Cependant la manipulation devient lourde et fastidieuse... La démarche m'apparait toutefois intéressante car on obtient des classes > 1 et des fractions dont les numérateurs ne sont pas forcément facteurs de 24.

Ex: $(\frac{18}{24}, \frac{144}{24}, \frac{16}{8}, \ldots)$



A cause de l'unité de base choisie on ne peut pas engendrer de nouveaux états vers la droite ou vers le bas.

2.2 Buts didactiques

Un tel groupement, je crois, peut donner à l'enfant une idée de ce qu'est un rationnel (classe de fractions) et de ce que sont les fractions équivalentes.

Ainsi $\frac{3}{6}$ et $\frac{2}{4}$ sont dites équivalentes parce qu'on peut partant de 1 (par exemple) aller à $\frac{1}{2}$ par deux chemins $\left[1 \to \frac{1}{3} \to \frac{1}{6} \to \frac{3}{6}\right]$ ou $\left[1 \to \frac{1}{2} \to \frac{1}{4} \to \frac{2}{4}\right]$ etc.

Il serait sûrement intéressant de faire découvrir aux enfants qu'une opération peut être effectuée sur n'importe quel représentant d'une classe et que le résultat demeure le même

Ex: $\frac{1}{4} \xrightarrow{\times\frac{1}{3}} \frac{1}{12}$ ou $\frac{3}{12} \xrightarrow{\times\frac{1}{3}} \frac{1}{12}$ ou $\frac{6}{24} \xrightarrow{\times\frac{1}{3}} \frac{1}{12}$

$\frac{1}{4} \times \frac{1}{3} = \frac{1}{12}$ $\quad$ $\frac{3}{12} \times \frac{1}{3} = \frac{1}{12}$ $\quad$ $\frac{6}{24} \times \frac{1}{3} = \frac{1}{12}$

Cette prise de conscience sera utile pour effectuer les additions de fractions à dénominateur différent.

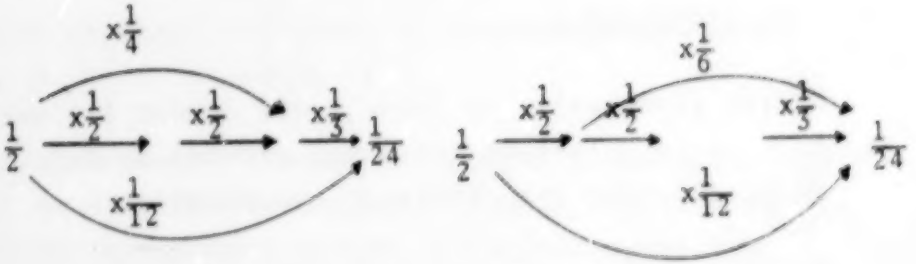
Ce groupement peut servir aussi à illustrer les lois des opérateurs multiplicatifs.

-commutativité de la x : (au niveau des opérateurs) considérons les deux chemins suivants menant de $\frac{1}{2}$ à $\frac{1}{12}$

$\frac{1}{2} \xrightarrow{\times\frac{1}{2}} \xrightarrow[\times\frac{1}{6}]{} \xrightarrow{\times\frac{1}{3}} \frac{1}{12}$ et $\frac{1}{2} \xrightarrow{\times\frac{1}{3}} \xrightarrow[\times\frac{1}{6}]{} \xrightarrow{\times\frac{1}{2}} \frac{1}{12}$

$\frac{1}{2} \times \frac{1}{3} = \frac{1}{3} \times \frac{1}{2} = \frac{1}{6}$

Ex:



$(\frac{1}{2} \times \frac{1}{2}) \times \frac{1}{3}$ $\qquad$ $\frac{1}{2} \times (\frac{1}{2} \times \frac{1}{3})$

$\frac{1}{4} \times \frac{1}{3}$ $\qquad$ $\frac{1}{2} \times \frac{1}{6}$

$\frac{1}{12}$ $\qquad = \qquad$ $\frac{1}{12}$

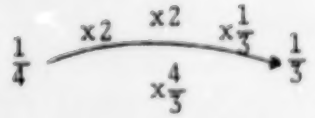
-opérateur neutre pour x :

Recherche du chemin direct permettant d'aller par exemple de $\frac{1}{4}$ à $\frac{1}{4}$.

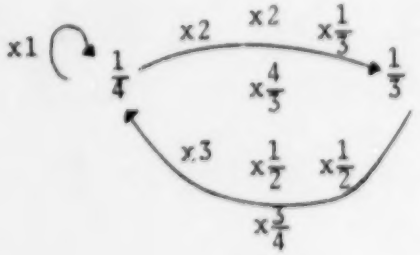
$$\frac{1}{4} \times 1 = \frac{1}{4}$$

-opérateur inverse pour x :

Chaque chemin possède son chemin inverse.
Considérons une série de chemins de $\frac{1}{4}$ à $\frac{1}{3}$, par exemple:



revenons à $\frac{1}{3}$ en empruntant le même chemin



Emprunter le chemin $x\frac{4}{3}$ suivi du chemin $x\frac{3}{4}$ (chemin inverse) revient à faire le chemin x1.

Ce groupement, nous l'avons vu, permet d'exploiter le concept de fraction équivalente (aspect fraction-état). Dans un tel groupement où les opérations consistent à multiplier par un élément de Q, il est aussi possible de mettre en évidence la fraction équivalente (aspect fraction-opérateur) en cherchant, par exemple, les chemins de $\frac{1}{4}$ à $\frac{1}{3}$, c'est-à-dire:

$\frac{1}{4} \times \square = \frac{1}{3}$

$\frac{1}{4} \xrightarrow[x\frac{4}{3}]{x2 \quad x2 \quad x\frac{1}{3}} \frac{1}{3}$ 1er chemin

$\frac{1}{4} \xrightarrow[x\frac{8}{6}]{x\frac{1}{2} \quad x\frac{1}{3} \quad x2 \quad x2 \quad x2} \frac{1}{3}$ 2e chemin plus long que le 1er mais équivalent au 1er.

etc...

Une telle démarche, je crois, permettrait de trouver des classes d'opérateurs (chemins) équivalents.

Cette situation $\frac{1}{4} \boxed{x\frac{4}{3}} = \frac{1}{3}$ est en fait le problème suivant:

-par quoi multiplier $\frac{1}{4}$ pour obtenir $\frac{1}{3}$

-ou $\frac{1}{3} \div \frac{1}{4} \times \frac{4}{3}$: c'est ici que je constate que la recherche de la représentation réduite d'un groupement me fait voir de nouvelles possibilités ou notions que "cache" un groupement.

Comme les actions élémentaires de ce groupement consistent à prendre $\frac{1}{2}$ et $\frac{1}{3}$ où 2 et 3 sont facteurs premiers de 24, je crois qu'il serait possible d'exploiter dans un tel groupement la notion de fraction irréductible en exprimant numérateur et dénominateur par un produit de facteur premier.

Voir graphe p. 140.

Exemple: $\frac{18}{24} = \frac{3 \times 3 \times 2}{2 \times 2 \times 2 \times 3}$ (suivre les flèches ... de $\left[\frac{1}{24}\right]$ à $\left[\frac{18}{24}\right]$ (suivre les flèches → de $[1]$ à $\left[\frac{1}{24}\right]$

recherche du PGCD

$$\frac{18}{24} = \frac{3 \times (3 \times 2)}{2 \times 2 \times (2 \times 3)} = \frac{3}{4}$$

Dans cette deuxième partie du travail, je n'ai que signalé les notions (ou sous notions) visées par un tel groupement. Le plus "difficile" reste à faire: penser une approche possible qui permettrait d'exploiter au maximum les possibilités d'un tel groupement.